PROSPETTIVE PENALISTICHE DEL CONTROLLO A DISTANZA SULL'ATTIVITÀ LAVORATIVA NELL'ATTUALE CONTESTO NORMATIVO E TECNOLOGICO (*)

di Attilio Nisco

L'art. 4 della L. n. 300/1970 (Statuto dei Lavoratori) è tuttora considerato un baluardo a tutela della dignità e della riservatezza del lavoratore rispetto ai controlli a distanza esercitabili dal datore di lavoro. La sua recente riscrittura ha determinato effetti sulla connessa fattispecie penale, confluita nell'art. 171 del d.lgs. 196 del 2003 (c.d. Codice Privacy). Il presente lavoro intende analizzare la fattispecie penale, mostrandone la complessiva indeterminatezza, emergente soprattutto dal rapporto tra sua attuale formulazione ed impiego di tecnologie idonee sì a conseguire un controllo a distanza del lavoratore, eppure estremamente diffuse (e in certi casi indispensabili) nell'esercizio dell'attività lavorativa. In tale prospettiva diviene essenziale, anche in chiave penalistica, chiarire quali strumenti di potenziale controllo a distanza siano esenti dalle autorizzazioni previste dall'art. 4 St. lav. e quale sia la natura penalistica di tali esenzioni. È inoltre necessario considerare l'eventuale spazio applicativo di istituti scriminanti di problematico inquadramento, come i c.d. "controlli difensivi", anche in accordo con la giurisprudenza della Corte EDU in materia. Infine, il contributo si sofferma sui nessi tra controlli a distanza e responsabilità amministrativa degli enti, distinguendo i profili attinenti alla predisposizione di modelli organizzati ante delictum da quelli connessi all'attività di indagine interna all'ente, disposta successivamente al verificarsi di un'infrazione. Con riferimento a tale ultima ipotesi, nell'ottica dell'introduzione di una disciplina organica delle indagini interne, viene evidenziato il problematico coordinamento tra tutela dei lavoratori e diritto di difesa dell'ente.

(*) Il contributo si colloca nell'ambito del Progetto di Ricerca PRIN 2017EC9CPX "Dis/Connection: Labor and Rights in the Internet Revolution", a cui partecipano le Università di Bologna, Napoli Federico II, Udine, Venezia Ca' Foscari.

1. Premessa: breve retrospettiva e ragioni di un rinnovato interesse penalistico per l'art. 4 St. lav.

Il controllo datoriale a distanza può oggi perseguire molteplici canali: dall'accesso ai sistemi informatici aziendali alla navigazione in *internet*, dalla corrispondenza via mail alla presenza sui *social network* [1]. A tali possibilità tecnologiche ha corrisposto un'evoluzione della normativa (anche penale) in materia di riservatezza, a tutela del lavoratore come di qualunque consociato.

In tale contesto, permane la specifica tutela del lavoratore dai controlli a distanza, che trova tuttora il proprio caposaldo nell'art. 4 St. lav. (l. 300/1970). Definita «una delle più efficaci dimostrazioni della lungimiranza del legislatore statutario»[2], la norma ha subìto modifiche volte a farle reggere il passo con la suddetta evoluzione[3]. Al tempo stesso, essa è diventata snodo di intricate questioni, che non riguardano solo i suoi nessi (palesi) con la *privacy*, ma anche una serie di interazioni con il sistema penale non ancora adeguatamente colte dal legislatore, come si confida di dimostrare.

Prima di addentrarci nell'analisi della normativa vigente, è opportuno riepilogare i lineamenti essenziali della vecchia fattispecie[4].

Il testo originario dell'art. 4 St. lav. contemplava due distinte fattispecie di reato, assoggettate allo stesso trattamento sanzionatorio, in corrispondenza di due distinte forme di controllo: i controlli "intenzionali", consistenti in una deliberata sottoposizione dell'attività lavorativa ad un controllo a distanza senza altri scopi legittimi, ed i controlli che, secondo la dizione (atecnica) invalsa tra i giuslavoristi, si definiscono "preterintenzionali", in quanto discendenti dall'installazione quale sua conseguenza accidentale, cioè inevitabile ma non direttamente voluta dal datore[5].

In base al primo comma dell'art. 4 era punita la violazione del divieto assoluto di controlli intenzionali, ovvero "l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori", secondo i canoni di un reato di pericolo concreto, per il quale non era necessario appurare che all'uso seguisse

---

[1] Sul tema PECORELLA, DE PONTI (2011), GROTTO (2014), p. 57 ss.

[2] ZILIO GRANDI, PETTINELLI (2020), p. 2.

[3] La letteratura relativa all'art. 4 St. lav., anche dopo la riforma, resta imponente; senza pretese di esaustività, si veda: DAGNINO (2015), p. 988 ss.; ALVINO (2016); CARINCI (2016), RUSSO (2016), DEL PUNTA (2016) p. 77 ss. MARESCA (2016), p. 513 ss.; PROIA (2016), p. 547 ss.; TEBANO (2016); p. 345 ss.; ZOLI (2016), p. 635 ss. CASSANO (2020) p. 778 ss.; FABOZZI (2020), p. 54 ss.; ZILIO GRANDI, PETTINELLI (2020), p. 1 ss.

[4] Per un commento di taglio penalistico alla vecchia disposizione, PADOVANI (1985), p. 252 ss. Nel quadro di una più ampia indagine sui profili penalistici della l. 300/1970, v. STORTONI (1974), p. 1419 ss. (prendendo spunto dall'attualità di tale saggio, v. anche CURI (2015), p. 503 ss.). In tempi più recenti, ARENA, CUI (2012), p. 212 ss.; PECORELLA, DE PONTI (2011), p. 21 ss. Per una complessiva retrospettiva sull'art. 4, FABOZZI (2020), p. 59 ss.

[5] Cfr. ROMAGNOLI (1972), p. 16 ss. Sul carattere convenzionale del termine "preterintenzionale" si sofferma MARESCA (2016), p. 518; sull'utilizzo "fuorviante" di questo termine, DEL PUNTA (2016), p. 81.

l'effettivo controllo, ma piuttosto il fatto che lo strumento fosse oggettivamente predisposto ed anche prossimo a conseguire la finalità vietata.

Il secondo comma, invece, si riferiva ad "impianti ed apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori". La relativa istallazione necessitava di un accordo con le rappresentanze sindacali aziendali o, in mancanza di queste, con la commissione interna, oppure, in difetto di accordo e su istanza del datore di lavoro, di un provvedimento dell'Ispettorato del lavoro. La correlata fattispecie penale sanzionava l'istallazione in assenza di tali presupposti, atteggiandosi a reato di pericolo astratto, posto che ad esser punita era la mera "possibilità" di un controllo, insita nell'istallazione in difetto dell'accordo o dell'autorizzazione.

Sul piano formale, il secondo comma appariva come una facoltà ritagliata sul divieto generale posto dal primo comma. Ma che si trattasse di un reato distinto, benché punito allo stesso modo di quello previsto dal primo comma, era dimostrato dall'eterogeneità delle condotte descritte dai due commi, modellate su «comportamenti privi di implicazione logica necessaria»[6]: da un lato, l'"uso" di impianti ed apparecchiature finalizzate al controllo; dall'altro, l'"istallazione" con "possibilità" di un controllo, a prescindere dall'effettivo utilizzo degli impianti. Proprio in virtù di questa eterogeneità, la disposizione di cui al secondo comma non era intesa a delimitare il perimetro della fattispecie contenuta al primo comma – in guisa di scriminante o di causa di non punibilità –, ma per l'appunto a delineare una fattispecie distinta dalla precedente[7].

La riforma del 2015 ha mutato questo assetto strutturale, concentrando la tutela penale in un'unica fattispecie, il cui contenuto va ora dedotto da tre distinte disposizioni (art. 171 Codice *Privacy* e artt. 4 e 38 St. lav.).

Sullo sfondo della modifica si celano almeno tre ordini di esigenze[8].

In primo luogo, la necessità di aggiornare la norma alle innovazioni tecnologiche intervenute (anche) nel mondo del lavoro, di cui è figlia una ridefinizione degli "strumenti" di controllo presi in considerazione. In secondo luogo, l'intento di rimediare ai contrasti provocati dal ricorso alla discussa categoria dei controlli "difensivi", aggiungendo la tutela del patrimonio aziendale alle esigenze legittimanti il controllo a distanza.

Infine, nell'ambito di un più generale riassetto dei rapporti con la normativa in materia di riservatezza, l'introduzione di una disciplina relativa all'utilizzabilità delle informazioni acquisite tramite il controllo.

Si tratta di aspetti non privi di ricadute penalistiche, le quali, come vedremo, travalicano i confini della stretta esegesi testuale dell'art. 4, da cui pure bisognerà prendere le mosse. Oltre che un esame sistematico della riformata fattispecie, dal quale emergeranno gli attuali limiti dell'intervento penale in materia, sarà necessario

---

[6] PADOVANI (1985), p. 253.

[7] PADOVANI (1985), p. 253.

[8] Seguiamo CAIRO, VILLA U. (2019), p. 676 ss.

soffermarsi sulle implicazioni, non meno problematiche, derivanti dalla convivenza dell'art. 4 St. lav. con la responsabilità degli enti *ex* d.lgs. 231/2001.

2. La vigente fattispecie penale e la sua contorta previsione.

Per effetto delle modifiche apportate dall'art. 23 d.lgs. 151/2015 (nel quadro del c.d. *Jobs Act*) e poi dall'art. 5, comma 2 d.lgs.185/2016, l'art. 4 St. lav., originariamente rubricato "Impianti audiovisivi", fa ora rifermento ad "Impianti audiovisivi e altri strumenti di controllo". La disposizione è stata riscritta e formalmente collegata all'art. 171, d.lgs. 196/2003 (Codice *Privacy*), che ha recepito la relativa contravvenzione.

Si è così innescato un complesso meccanismo di rinvii, tra Statuto dei lavoratori e Codice *Privacy*, che certo non giova alla ricostruzione del reato[9]. Né può essere ritenuta incisiva, da questo punto di vista, la più recente modifica dell'art. 171 Codice *Privacy*, indotta dall'art. 15, comma 1, lett. f), d.lgs. 101/2018, che, riferendo la sanzione penale alla sola violazione del primo comma dell'art. 4 St. lav., si è limitata a confermare la vigenza del reato[10] e ad emendare un difetto formale di raccordo tra le disposizioni interessate.

Più esattamente, l'art. 171 Codice *Privacy*, rubricato "violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori", stabilisce che "La violazione delle disposizioni di cui agli articoli 4, comma 1, e 8 della legge 20 maggio 1970, n. 300, è punita con le sanzioni di cui all'articolo 38 della medesima legge". Si tratta di una norma incriminatrice dalla conformazione alquanto singolare, dal momento che non descrive il comportamento incriminato né fissa la relativa sanzione, ma si limita a richiamare e a porre in relazione le disposizioni da cui trarre tali elementi. Per di più, mentre entrambe le disposizioni richiamate risultano collocate nello Statuto dei lavoratori, il loro collegamento avviene in un contesto normativo distinto, il d.lgs. 196/2003, dedicato ad una materia diversa, sia pure indubbiamente connessa ad alcuni profili disciplinati dallo statuto.

Una simile tecnica normativa non può certo incontrare il favore del penalista, per diverse ragioni[11].

Notiamo, anzitutto, come essa muova in senso opposto alla direttiva espressa dall'art. 3-bis c.p. (riserva di codice), ai sensi del quale "le disposizioni che prevedono reati possono essere introdotte nell'ordinamento solo se modificano il codice penale ovvero sono inserite in leggi che disciplinano in modo organico la materia". A prescindere dall'applicabilità *ratione temporis* dell'art. 3-bis c.p. alla fattispecie in commento, si rivelano qui tutte le difficoltà di individuazione di una nozione di legge "organica" da contrapporre, quale valida alternativa (nei termini di cui all'art. 3-bis c.p.),

---

[9] Per commenti aggiornati di taglio penalistico, v. CURI (2017), p. 181 ss.; FLOR (2016), p. 161 ss.; FURLOTTI (2019), p. 1502 ss.; MANNA, DI FLORIO (2019), p. 924 ss.

[10] Cfr. Cass. pen., sez. III, 14 dicembre 2020, n. 3255, in *DeJure*.

[11] Cfr. i rilievi critici di CURI (2017), *passim*.

all'inserimento nel Codice penale di una (nuova) incriminazione[12]. La previsione del reato che ci occupa è addirittura sita a cavaliere di due testi legislativi, quasi a voler sconfessare l'esistenza, o comunque a compromettere la ricostruzione, di una disciplina organica della materia.

Soprattutto, è resa ardua la riconoscibilità del precetto che – per la parte che qui interessa – va tuttora ricavato dall'art. 4, comma 1 St. lav.

Caratteristica di quest'ultima norma è la sua enunciazione in termini che paiono attribuire una facoltà al destinatario (al datore di lavoro), in quanto, almeno apparentemente, le attività descritte non sono rese oggetto di divieto, ma risultano esercitabili in presenza dei presupposti normativamente indicati. Ciò ha indotto la dottrina a chiedersi se l'attuale formulazione abbia fatto venir meno il divieto di utilizzo di controlli intenzionali. Ad uno sguardo più attento, tale divieto risulta ancora vigente, benché espresso in maniera implicita[13]. Si dispone, infatti, che "gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza […] possono essere impiegati *esclusivamente*" per determinate finalità; dal che risulta vietato ogni impiego per *finalità diverse*, compresa la sottoposizione fine a se stessa dell'attività lavorativa ad un controllo a distanza.

Di tale avviso è anche la giurisprudenza penale, che su queste basi ravvisa una continuità intertemporale tra l'attuale fattispecie ed il reato originariamente punito dal combinato disposto degli artt. 4 e 38 St. lav.[14].

Ne risulta una fattispecie in palese attrito con il principio di legalità, in quanto le condotte penalmente sanzionate, più che essere espressamente descritte dalla norma, vanno desunte da ciò che essa non dice, cioè dal novero dei comportamenti datoriali non autorizzati o non autorizzabili[15]. In quest'ottica, risultano vietati l'impiego e l'istallazione di impianti audiovisivi e di altri strumenti di controllo, in mancanza di due ordini di requisiti[16]:

---

[12] Sul punto, si vedano le riflessioni di SEMINARA (2020), spec. § 1.2.

[13] Si tratta di lettura condivisa dalla prevalente dottrina giuslavoristica: v., ad es., ALVINO (2016), p. 16; FABOZZI (2020), pp. 79-80, ed ivi ulteriori riferimenti; in termini problematici, CARINCI (2017), p. 45 ss.

[14] V. Cass. pen., sez. III, 8 settembre 2016, n. 51897, in *DeJure*: «[…] con la rimodulazione dell'art. 4 dello Statuto dei Lavoratori, è solo apparentemente venuto meno il divieto esplicito di controlli a distanza, nel senso che il superamento del divieto generale di detto controllo non può essere predicato sulla base della mancanza, nel nuovo art. 4, di una indicazione espressa (com'era nel previgente art. 4, comma 1) di un divieto generale di controllo a distanza sull'attività del lavoratore, avendo la nuova formulazione solamente adeguato l'impianto normativo alle sopravvenute innovazioni tecnologiche e, quindi, mantenuto fermo il divieto di controllare la sola prestazione lavorativa dei dipendenti, posto che l'uso di impianti audiovisivi e di altri strumenti di controllo può essere giustificato "esclusivamente" a determinati fini, che sono *numerus clausus* (cioè per esigenze organizzative e produttive; per la sicurezza del lavoro e per la tutela del patrimonio aziendale) e alle condizioni normativamente indicate, sicché residua un regime protezionistico diretto a salvaguardare la dignità e la riservatezza dei lavoratori, la cui tutela rimane primaria nell'assetto ordinamentale e costituzionale, seppur bilanciabile sotto il profilo degli interessi giuridicamente rilevanti con le esigenze produttive ed organizzative o della sicurezza sul lavoro».

[15] V. i rilievi di FLOR (2016), p. 170.

[16] Cfr. MARESCA (2016), p. 519.

- un requisito di carattere sostanziale inerente all'*impiego* dello strumento, riconducibile ad una delle tre esigenze tassativamente indicate dalla norma (intese come scopi in senso oggettivo del controllo, non come mere finalità soggettivamente perseguite dal datore): esigenze organizzative e produttive, sicurezza del lavoro, tutela del patrimonio aziendale;
- un requisito di carattere procedurale, in base al quale l'*istallazione* dello strumento deve essere preceduta dall'accordo con le associazioni sindacali o in subordine dall'autorizzazione dell'Ispettorato del lavoro.

Funzione di tali requisiti è garantire un bilanciamento tra potere datoriale di controllo e interessi del lavoratore[17], sì che, dal punto di vista penalistico, presupposti e forme dell'autorizzazione, letti ovviamente *a contrario,* configurano condizioni di illiceità espressa della condotta, operative già sul piano della tipicità; per converso, in presenza dei requisiti di forma e di sostanza dell'autorizzazione, il reato non sussiste per mancanza del fatto tipico.

3. La centralità del momento procedurale: conseguenze sulla tipicità ed offensività del fatto.

Resta la notevole ampiezza dei requisiti sostanziali ai quali deve essere asservito il controllo, per essere definito legittimo: di quelli già noti alla disposizione, vale a dire le esigenze aventi a che fare con l'organizzazione, la produzione e la "sicurezza del lavoro" (formula, quest'ultima, non coincidente con la sicurezza trattata dal d.lgs. 81/2008), come pure del requisito di più recente introduzione, ravvisato nella tutela del patrimonio aziendale.

È dato allora rilevare che il momento procedurale prenda il sopravvento nell'economia della fattispecie, nel senso che, sulla reale conformità del controllo agli scopi riconosciuti dalla norma – e quindi, in ultima istanza, sui confini del comportamento lecito –, sarà decisivo l'accordo sindacale o il provvedimento amministrativo, secondo le cadenze dettate dall'art. 4 St. lav. Ciò significa che il disvalore penalistico della condotta è sostanzialmente rimesso alla definizione di una fonte di rango sublegislativo o addirittura negoziale: con buona pace, oltre che della determinatezza, del principio di riserva di legge[18].

Senza contare che la tipicità risulta ulteriormente sfibrata dalla natura contravvenzionale del reato, permeabile all'imputazione colposa, sì che l'agente risulterà punibile anche a causa di una involontaria infrazione dell'accordo sindacale o delle prescrizioni contenute nel provvedimento autorizzativo. Se poi si considera che la disposizione tiene distinti "impiego" e "istallazione", e che i requisiti di liceità delle due condotte sono espressi in forma cumulativa (cosicché la punibilità potrà dipendere dal difetto anche di uno solo di essi), si ottiene una gamma piuttosto variegata

[17] V., per tutti, DEL PUNTA (2016), p. 78.
[18] FLOR (2016), p. 171.

di condotte punibili, assoggettate, per altro, alla medesima sanzione (modulabile, comunque, in base ai criteri stabiliti dall'art. 38 St. lav.).

È innanzitutto punito un comportamento prodromico al controllo, qual è l'installazione, ossia la sola predisposizione di uno strumento di controllo senza la sua attivazione[19], allo stesso modo del suo impiego effettivo, che mette in concreto pericolo – o, secondo altre letture, offende – l'interesse del lavoratore. È inoltre punito l'impiego per esigenze diverse da quelle indicate dalla norma, anche qualora vi sia stato un accordo sull'istallazione (sul presupposto, invero non pacifico, che l'accordo possa essere assoggettato al sindacato del giudice)[20], come pure l'installazione in difetto di accordo o di autorizzazione, anche qualora di fatto il datore abbia agito per soddisfare una delle esigenze indicate, ed anche là dove lo strumento non sia stato effettivamente impiegato.

In tal modo, installazione e impiego (vietati) non sono più termini di riferimento di due fattispecie eterogenee, come avveniva in passato[21], bensì modalità di realizzazione di un unico reato, che assume le sembianze di norma a più fattispecie. Inoltre, il reato resta unico anche se la condotta si protrae nel tempo, considerando che, mentre l'installazione corrisponde ad una condotta istantanea, l'impiego di uno strumento può essere reiterato, dando vita ad un reato di durata[22].

La polarizzazione del disvalore delle condotte incriminate attorno all'assenza di un atto autorizzativo fa luce sulla reale natura degli interessi protetti dalla disposizione in commento. Lo statuto colloca l'art. 4 tra le norme a tutela della libertà e dignità del lavoratore, mentre i più recenti interventi lo avvicinano – o lo assimilano – alla tutela della riservatezza. Ma sul piano penalistico queste formule non sono appaganti, trattandosi di stabilire quale sia il bene giuridico del corrispettivo reato.

L'impiego del termine "dignità" per indicare un bene giuridico penalmente tutelato necessiterebbe di precisazioni inaffrontabili in questa sede, né parrebbe immediatamente compatibile con il meccanismo autorizzativo configurato dall'art. 4 St. lav. (davvero l'Ispettorato è chiamato a decide della "dignità" del lavoratore?)[23]. Viceversa, la riservatezza, al di là dei suoi sviluppi e declinazioni, si presta meglio a rivestire questo ruolo, tanto più alla luce della riforma che ha ricollocato il reato *de quo* nell'ambito del Codice *Privacy* [24].

---

[19] Cfr. Cass. pen., sez. III, 7 aprile 2016, n. 45198, in *DeJure*.

[20] Se l'accordo sindacale (o il provvedimento amministrativo) consentisse modalità di controllo oggettivamente lesive della dignità del lavoratore, il reato potrebbe configurarsi, là dove l'accordo (o provvedimento) fosse da considerare nullo o giuridicamente inesistente, in analogia a quanto accade per altri reati basati sulla mancanza di un'autorizzazione.

[21] V. *supra*, § 1.

[22] Cfr. Cass. pen., 8 settembre 2016, n. 51897, cit., che classifica la fattispecie in commento come «reato eventualmente abituale».

[23] In passato, invero, la dignità del lavoratore è stata colta come emanazione della sua libertà personale: v. ROMAGNOLI (1972), p. 17; lo stesso A. rivelava, per altro, la decisione dell'Ispettorato del lavoro poteva (e può) essere richiesta solo dal datore, sì da non prendere in considerazione gli interessi dei lavoratori, ma in base all'interesse pubblico (ROMAGNOLI (1972), pp. 20-21).

[24] Sia pure alla luce dell'evoluzione subita dal concetto di riservatezza, FLOR (2016), p. 173 ss. Le specifiche esigenze di protezione della riservatezza sui luoghi di lavoro vengono tuttora evidenziate dalla dottrina

Tuttavia, se la riservatezza fosse davvero il bene giuridico protetto dalla norma in commento, dovrebbe discenderne la disponibilità attraverso il consenso del titolare[25], cioè del lavoratore sottoposto al controllo: ma a parte un isolatissimo precedente[26], la giurisprudenza è oramai ferma nel rilevare l'inefficacia scriminate del consenso formalmente espresso (anche per iscritto) da tutti i lavoratori, ritenendo che la procedura prevista dalla norma statutaria sia inderogabile[27].

Più esattamente, la Corte di cassazione individua nella procedura un modo per affidare la composizione degli interessi in gioco alle rappresentanze sindacali o, in subordine, ad un organo pubblico, escludendo che i singoli lavoratori possano autonomamente decidere, in quanto soggetti deboli del rapporto di lavoro subordinato, come tali esposti a possibili abusi[28]. La ragione a sfavore del consenso scriminante pare inappuntabile; ma sul piano sistematico ne risulta che l'oggetto immediato di tutela della norma penale in commento coincide con la *modalità di regolazione* degli interessi dei lavoratori, configurata dall'art. 4 St. lav. (e resa indisponibile ai singoli lavoratori), non con gli *interessi finali* regolati.

In altre parole: oggetto di tutela non è propriamente un "bene" ma una procedura, la quale, a tutto concedere, rappresenta un bene strumentale alla difesa di interessi individuali. Di conseguenza, rispetto a tali interessi, la fattispecie si atteggia a reato di pericolo astratto. Ed è questa l'unica ricostruzione capace di spiegare – non necessariamente di legittimare – l'equiparazione sanzionatoria tra installazione ed utilizzo delle apparecchiature: comportamenti caratterizzati da un diverso coefficiente di pericolosità rispetto ai beni finali, ma egualmente devianti dall'assetto procedurale precostituito dalla legge.

---

specialistica: cfr. PROIA (2016), p. 549 ss.

[25] Si vedano le considerazioni di SGUBBI (1998), p. 758, in sede di primo commento (penalistico) alla prima disciplina sulla *privacy*.

[26] Cass. pen., sez. III, 17 aprile 2012, n. 22611, in *DeJure*.

[27] Cass. pen., sez. III, 31gennaio 2017, n. 22148; sez. III, 10 aprile 2018, n. 38882; sez. III, 15 luglio 2019, n. 50919; sez. III, 16 novembre 2019, tutte in *DeJure*.

[28] Così Cass. pen., sez. III, 16 novembre 2019, cit.: «[…] in mancanza di accordo o del provvedimento alternativo di autorizzazione, l'installazione dell'apparecchiatura è illegittima e penalmente sanzionata. Questa procedura - frutto della scelta specifica di affidare l'assetto della regolamentazione di tali interessi alle rappresentanze sindacali o, in ultima analisi, ad un organo pubblico, con esclusione della possibilità che i lavoratori, *uti singuli*, possano autonomamente provvedere al riguardo - trova la sua ratio nella considerazione dei lavoratori come soggetti deboli del rapporto di lavoro subordinato. La diseguaglianza di fatto, e quindi l'indiscutibile e maggiore forza economico-sociale dell'imprenditore, rispetto a quella del lavoratore, rappresenta la ragione per la quale la procedura codeterminativa sia da ritenersi inderogabile (a differenza di quanto ritenuto invece dalla Sez. 3, n. 22611 del 17/04/2012), potendo essere sostituita dall'autorizzazione della direzione territoriale del lavoro solo nel solo di mancato accordo tra datore di lavoro e rappresentanze sindacali, non già dal consenso dei singoli lavoratori, poiché, a conferma della sproporzione esistente tra le rispettive posizioni, basterebbe al datore di lavoro fare firmare a costoro, all'atto dell'assunzione, una dichiarazione con cui accettano l'introduzione di qualsiasi tecnologia di controllo per ottenere un consenso viziato, perché ritenuto dal lavoratore stesso, a torto o a ragione, in qualche modo condizionante l'assunzione».

4. La problematica delimitazione degli strumenti di controllo.

In tale quadro si colloca una delle più importanti modifiche della norma statutaria: la riformulazione della nozione di strumento oggetto di impiego e installazione, nella quale, oltre agli "impianti audiovisivi", di cui faceva menzione anche la vecchia disposizione, rientrano anche "altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori".

In linea di continuità con la normativa precedente, il "controllo a distanza" comprende la distanza in senso sia fisico che cronologico. Può trattarsi cioè di impianti che permettono di sorvegliare il lavoratore da un luogo lontano dalla postazione (come accade con una telecamera) e/o di strumenti che consentono verifiche sull'attività non contemporanee allo svolgimento della prestazione (mediante registrazione di dati)[29].

Di ampiezza invariata resta l'oggetto del controllo, concernente l'"attività lavorativa", espressione «che supera il mero adempimento della prestazione e sembra voler abbracciare l'intero comportamento umano nel luogo di lavoro», esposto a rischi di intrusione per la natura stessa del rapporto di lavoro [30]. Non rileva comunque l'uso o l'installazione di impianti in luoghi non preposti allo svolgimento dell'attività.

Mutano invece sensibilmente i termini del rapporto tra il controllo e la natura dell'oggetto impiegato per esercitarlo.

Dall'art. 4 vigente si evince che «[…] il "controllo" non costituisce necessariamente la funzione primaria e tipica degli "strumenti" a cui il legislatore si riferisce, ma identifica le capacità di cui lo strumento è "anche" dotato» [31]. La circostanza è di per sé produttiva di significative conseguenze penalistiche, non tanto sul fronte dell'offensività, quanto su quello della legalità della fattispecie. Infatti, con riguardo all'offensività, già il vecchio art. 4 (comma 2) si assestava sulla soglia del pericolo astratto, punendo la mera installazione, non per forza seguita da un effettivo utilizzo dello strumento; solo che, in quel contesto, il pericolo poteva dirsi ragionevolmente presunto da una caratteristica oggettiva dello strumento (costituita dalla sua funzione tipica), mentre adesso andrà dedotto soprattutto dal suo possibile utilizzo quale strumento "anche" di controllo.

Senonché, nel passaggio dalla dizione "apparecchi" (di controllo) a "strumenti" (di potenziale controllo), è la sostanza stessa dell'oggetto su cui cade la condotta a decomporsi, in termini problematici soprattutto dal punto di vista della tipicità.

A tal proposito, sul presupposto che la *ratio* manifesta di questa estensione del mezzo con cui si realizza la condotta sia la necessità di adattare la norma alle nuove forme di controllo tecnologico, una dottrina esperta ha ravvisato significative analogie con la tecnica normativa collaudata nel diritto penale dell'informatica: la locuzione "altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori" finisce col rappresentare «una sorta di clausola aperta», capace di ricomprendere «ogni mezzo, fisico o logico, *hardware* o *software*, connesso o meno con un

[29] RUSSO (2016), p. 6; ZOLI (2016), p. 639.
[30] RUSSO (2016), p. 7.
[31] MARESCA (2016), p. 519.

sistema di elaborazione dati o in rete, che consenta anche solo la possibilità di attivare un controllo a distanza» [32].

Sul punto interviene anche il comma 2 dell'art. 4, che prevede delle esenzioni dal regime sancito dal comma 1.

Sono anzitutto esentati gli strumenti di registrazione degli accessi e delle presenze, che il legislatore ha inteso escludere dalla disciplina di cui al primo comma onde risolvere una disputa relativa alla necessità di autorizzare tali strumenti, il cui funzionamento implica una registrazione di dati concernenti l'attività lavorativa. La formula legislativa pone un'unica questione interpretativa: se cioè il termine "presenze" includa anche gli spostamenti del dipendente all'interno dei luoghi di lavoro, sì che risulterebbe esente da autorizzazione l'impiego di strumenti idonei a monitorare la mobilità del lavoratore rispetto alla sua postazione[33]. Nell'ottica penalistica, pare preferibile la tesi che reputa esenti da autorizzazione solo gli strumenti, in senso stretto, finalizzati a rilevare l'accesso, dal momento che allo stesso strumento potrebbero essere aggiunti congegni eccessivamente limitativi della *privacy* del lavoratore[34].

Più complesso definire la categoria degli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa; definizione che deve prescindere da una distinzione tra organizzazione ed esecuzione della prestazione[35]. Diviene qui evidente il superamento della dicotomia tra strumento di controllo e strumento di lavoro e, al tempo stesso, un aggiornamento di quest'ultima nozione. Lo strumento di lavoro non è più solo quello individualmente assegnato al dipendente, ma può essere costituito, ad esempio, dall'interazione con un sistema informatico aziendale centralizzato, utilizzato dal dipendente tramite una connessione periferica attraverso un dispositivo fisso o mobile[36].

Prima di esaminare i possibili contenuti di siffatta esenzione, occorre interrogarsi sulla funzione sistematica da essa assolta dal punto di vista penalistico.

Il comma 2 dell'art. 4 dispone, testualmente, che il comma 1 "non si applica" nelle suddette ipotesi; il che significa che gli strumenti di controllo di cui al comma 2, non solo sono esclusi dall'autorizzazione, ma sono parimenti sottratti al regime sanzionatorio di cui all'art. 38 St. lav. per il tramite dell'art. 171 Codice *Privacy* (conclusione logica, anche prima della modifica intervenuta nel 2018). Ci si può chiedere, allora, se tale effetto sia dovuto all'operatività di una causa di esclusione del tipo, di una causa di giustificazione o di una causa di non punibilità[37].

La prima qualifica sembra la più appropriata. L'esenzione, difatti, non deriva da una ragione di mera opportunità, a cui è solitamente connessa una causa di non punibilità, che per altro interviene al cospetto di un reato perfetto in tutti i suoli elementi:

---

[32] FLOR (2016), p. 167.

[33] Cfr. MARESCA (2016), p. 536 ss.; CAIRO, VILLA U. (2020).

[34] Così, MANNA, DI FLORIO (2019), p. 928-929, i quali fanno l'esempio di un *badge* dotato di tecnologia RFID (*Radio Frequency Identification Device*), il cui impiego potrebbe addirittura preludere ad una violazione dell'art. 8 St. lav.

[35] Su tali aspetti, diffusamente, MARESCA (2016), p. 532 ss.

[36] Cfr. nuovamente MARESCA (2016), pp. 532-533.

[37] Sulla distinzione, CONSULICH (2018), p. 183 ss.

situazione che non ricorre nel caso disciplinato dal comma 2. Né a fondamento dell'esenzione sembra potersi ravvisare un bilanciamento tra opposti interessi, uno dei quali ulteriore rispetto a quelli protetti dal comma 1, che "giustifichi" – in senso tecnico – la lesione della dignità e della riservatezza del lavoratore (o, come visto sopra, della funzione strumentale alla loro tutela). Piuttosto, con la disposizione di cui al comma 2, si riconosce la *liceità di fondo* degli strumenti ivi considerati[38], rispetto ai quali sarebbe eccessivamente gravoso o finanche irrealistico pretendere un'autorizzazione preventiva, dato il legame acquisito con l'organizzazione del lavoro e, soprattutto, con l'adempimento della singola prestazione.

Letta in chiave penalistica, la norma esprime così la necessità di meglio definire il concetto di "strumento" quale elemento costitutivo della fattispecie. Del resto, essa non allude a strumenti strutturalmente diversi da quelli presi in considerazione nel comma 1, bensì distinti sul piano funzionale, di tal che, se non ci fosse il comma 2, essi potrebbero essere ricondotti al novero dei mezzi utilizzabili per commettere il reato. In altri termini, siamo innanzi ad una clausola che delimita "in negativo" i mezzi potenzialmente idonei a realizzare il reato in ragione della funzione esplicata.

Ciò premesso, permangono insuperabili perplessità sulla reale capacità della formula legislativa di soddisfare tale scopo e quindi di contribuire alla determinatezza della fattispecie penale.

5. Innovazione tecnologica e (in)determinatezza della fattispecie.

La categoria degli "strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa", che assume importanza centrale nell'ambito della disposizione in commento, impone un considerevole sforzo esegetico. La dottrina giuslavoristica evidenzia, anzitutto, come non esista una nozione oggettiva di strumento finalizzato alla prestazione[39]. Perché possa parlarsi di "utilizzazione", dovrebbe essere riscontrata una partecipazione attiva del lavoratore nella relazione con lo strumento: nel senso che, ai fini dell'esonero dall'autorizzazione, parrebbe necessario che il lavoratore compia un'azione affinché lo strumento entri in funzione, e che sia messo al corrente degli effetti che discendono dall'impiego dello strumento. Se poi ne segue l'attivazione di un diverso dispositivo di controllo, con il quale il lavoratore non interagisce direttamente, occorrerà per esso l'autorizzazione richiesta dal comma 1.

Non è chiaro, invece, quale nesso debba intercorrere tra strumento e prestazione lavorativa, se cioè la formula impiegata dal legislatore vada intesa nel senso che lo strumento debba essere solo *utile* o anche *necessario* (se non indispensabile) all'esecuzione della prestazione[40].

Una parte della dottrina propende per un nesso di carattere *funzionale*: pur non essendo richiesto che l'utilizzo dello strumento sia condizione necessaria all'esecuzione

---

[38] DEL PUNTA (2016), p. 99.

[39] TULLINI (2017), p. 104 ss., con ulteriori riferimenti.

[40] Sulle incertezze suscitate dalla norma, ZOLI (2016), p. 644 ss.

della prestazione, si considera essenziale «*una stretta correlazione tra gli strumenti tecnologici e le mansioni svolte dal lavoratore*», di tal che lo strumento sia chiamato a rendere la prestazione più sicura o efficiente, ed il suo impiego a non "eccedere" i limiti della prestazione[41]. Segue però la precisazione secondo cui, ai fini dell'esenzione dall'autorizzazione sindacale o amministrativa, non pare sufficiente un impiego diretto solo al miglioramento dell'organizzazione (che ricadrà nella procedura prevista dal comma 1), per quanto da esso potrebbero discendere ripercussioni positive sulla produttività e, in ultimo, sull'efficacia della prestazione stessa[42]. Per tanto, pur essendo logicamente plausibile, il criterio funzionale non pare agevolmente praticabile.

5.1. Strumenti di lavoro e tecnologie informatiche: una breve rassegna.

Le difficoltà s'inspessiscono innanzi alle tecnologie informatiche, per la connaturata capacità degli elaboratori di conservare tracce del loro utilizzo – dunque dell'attività lavorativa – e, in caso di connessione *internet*, di permettere un controllo sulla cronologia della navigazione[43].

Va ricordato, a tal proposito, che la nozione di "strumento" richiede una distinzione tra componenti *hardware* e *software*: sì che, nel caso in cui al lavoratore sia assegnato un computer o un tablet, pur necessari allo svolgimento delle sue mansioni, i programmi ivi installati non possono ritenersi automaticamente esentati dall'autorizzazione, per così dire, per "incorporazione", là dove comportino un controllo non funzionale alla prestazione e/o di cui il lavoratore non sia partecipe, nei termini suddetti. Alla luce di tale premessa, il ricorso ad alcune tecnologie, oramai impiegate con grande frequenza nell'attività lavorativa, non può prescindere da un delicato giudizio casistico.

Così, ad esempio, è stato considerato strumento di controllo non strettamente funzionale alla prestazione un *proxy* di navigazione, installato sul computer aziendale, che consenta al datore di lavoro di tenere traccia delle informazioni inerenti alle navigazioni degli utenti della rete aziendale, con conseguente necessità di autorizzazione e del rispetto dell'obbligo di informazione di cui all'art. 4, comma 3 dello Statuto[44].

---

[41] R. DEL PUNTA (2016), p. 100 (corsivo nell'originale).

[42] DEL PUNTA (2016), p. 101.

[43] SITZIA (2017), p. 804 ss.; in prospettiva penalistica, MANNA, DI FLORIO (2019), p. 26 ss.; *ante Jobs Act*, PECORELLA, DE PONTI (2011).

[44] Così Trib. Torino (lav.), in *Riv. it. dir. lav.*, 2019, II, p. 3 ss., con commento di CRISCUOLO (2019), p. 9 ss. Nella motivazione si legge: «[…] il pc aziendale genericamente inteso, e quindi comprensivo anche della memoria di massa nonché del *software* (*browser*) necessario alla navigazione, costituisce strumento che, pur non avendo finalità di controllo ma finalità lavorativa, consente anche il controllo a distanza dell'operato del lavoratore, nei limiti in precedenza illustrati (*id est*: nesso di strumentalità tra il controllo e le esigenze tipizzate al comma 1, obbligo di informativa e rispetto delle codice della *privacy* di cui al comma 3). Per quanto invece concerne lo strumento denominato *proxy* di navigazione, è evidente come il medesimo, non essendo necessario [al lavoratore] per eseguire correttamente la propria attività lavorativa, più che

Più complessa diviene la distinzione tra strumento di lavoro e strumento di controllo, quando un unico *software* è utilizzato per l'attività lavorativa, ma risulta munito di una funzione integrata che consente il simultaneo controllo sull'efficienza della prestazione: si è osservato che, se quest'ultima funzione acquisisce "autonomia" e "specifica operatività" rispetto alle funzioni connesse alla prestazione – secondo una verifica non agevole sul piano tecnico –, servirebbero i requisiti procedurali previsti dall'art. 4, comma 1[45].

Incertezze suscita anche l'impiego di una piattaforma *software* per la registrazione delle telefonate intercorse tra lavoratori e clienti[46]. Sul presupposto che si tratti di uno strumento distinto dall'apparecchio telefonico, occorre anche qui valutare se prevalga la sua funzionalità all'adempimento della prestazione o se ricorrano esigenze organizzative o produttive che necessitano dell'autorizzazione sindacale (senza dimenticare che in alcuni casi, ad esempio nei contratti di borsa o di fornitura di alcuni servizi, la registrazione della telefonata costituisce adempimento di un dovere imposto dalle autorità di vigilanza)[47].

Una valutazione caso per caso si impone anche rispetto all'impiego di un sistema di navigazione GPS, che consenta la geolocalizzazione e la tracciabilità degli spostamenti del lavoratore. Si è argomentato che, se ad esempio il dispositivo è montato sull'automezzo di un dipendente addetto al servizio di ritiro e consegna di pacchi, dovrebbe rientrare nella deroga di cui al comma 2, trattandosi di strumento essenziale allo svolgimento della mansione. Diversamente, nel caso in cui il dispositivo serva solo a prevenire il furto di un veicolo aziendale, o nel caso in cui la mobilità territoriale non rientri nelle mansioni, l'installazione necessiterebbe dell'autorizzazione di cui al comma 1, sempre che ricorrano le ragioni ivi previste[48].

Problematico appare, infine, l'utilizzo dei *social network* per monitorare l'attività lavorativa, passibile, secondo una recente ricostruzione, di tre distinte qualificazioni [49].

---

rappresentare uno strumento di lavoro, risponda a prevalenti esigenze di controllo, essendo stato impiegato dalla società datrice di lavoro per ottenere informazioni relative alla navigazione Web da parte del dipendente, di talché il suo utilizzo richiede l'accordo con le organizzazioni sindacali o, in mancanza, l'autorizzazione dell'autorità amministrativa e, inoltre, deve essere ricondotto alle esigenze (diverse da quella di controllare l'esatto adempimento delle obbligazioni derivanti da rapporto di lavoro) previste dal primo comma dell'art. 4».

[45] MARESCA (2016), p. 536.

[46] Per un caso in cui è stata esclusa la natura di controllo a distanza, Trib. Pescara (lav.), 25 ottobre 2017, in *Riv. it. dir. lav.*, 2018, p. 307 ss., con nota di NUZZO (2018), p. 307 ss.

[47] MARESCA (2016), p. 534.

[48] Cfr. ALVINO (2016), p. 25; MARESCA (2016), p. 534. Per un caso di violazione (anche) dell'art. 4 l. 300/1970, v. il Provvedimento del 19 luglio 2018 del Garante per la protezione dei dati personali (in *www.garanteprivacy.it*), in merito all'installazione di GPS ed impianto di videosorveglianza su veicoli aziendali impiegati nel servizio di raccolta e trasporto di rifiuti. Va altresì segnalato il caso in cui le parti sottoscrivano un accordo, convenendo sulla qualifica di strumento di lavoro di un sistema GPS, nel caso in specie, corredato dalla Scoober App, utilizzati per tracciare l'attività dei c.d. riders. Si è al riguardo rilevato come l'art. 4 St. lav. sia norma imperativa ed inderogabile, che non consente alle parti di definire lo strumento di lavoro, sottraendolo alla valutazione dei soggetti indicati dal primo comma (INGRAO (2021) p. R.165 ss.).

[49] Seguendo ROCCHINI (2019), p. 143 ss.

Si rientrerebbe nell'utilizzo di uno strumento di lavoro, quando il *social network* sia impiegato per incrementare la comunicazione interaziendale, sì da rendere legittimo il controllo dell'attività senza la procedura autorizzativa. Una diversa qualificazione si profila, quando l'azienda si avvalga di una «comunità virtuale per finalità connesse al business, l'utilizzo della quale, tuttavia, non rappresenta un mezzo di esecuzione dell'attività di lavoro da parte dei prestatori», nel qual caso, il datore potrebbe accedere al social, ad esempio, per verificare eventuali anomalie nel traffico dei dati in internet idonee a causare il malfunzionamento della rete aziendale o la diffusione tramite la rete di informazioni aziendali riservate o compromettenti per l'immagine del datore. Di conseguenza, in tali ipotesi, il controllo potrebbe essere giustificato in quanto finalizzato alla tutela del patrimonio aziendale [50].

Controversa si prospetta soprattutto l'ultima ipotesi, riferita ad un utilizzo di *social network* per la tutela del patrimonio aziendale tramite profili *fake* appositamente costruiti dal datore per accertare le condotte illecite, ovviamente senza previa informazione al dipendente. Tale ipotesi è tata ricondotta dalla giurisprudenza alla categoria dei controlli "occulti" difensivi[51], di cui a breve ci occuperemo.

5.2. Mutamento del contesto della prestazione e dubbi sulla tenuta della fattispecie.

Gli esempi sopra riportati costituiscono solo una rassegna minima delle questioni che agitano il contenzioso del lavoro (e trovano riscontro nelle decisioni del Garante per la *privacy*), con riguardo soprattutto all'utilizzabilità in quella sede, *ex* art. 4, comma 3 St. Lav., delle informazioni reperite attraverso questo tipo di strumenti.

Al di là della corretta soluzione del singolo caso, è evidente che la logica casistica sia di per sé inconciliabile con il principio di tipicità[52]. Ma a parte questo rilievo, è forse necessario cominciare a considerazione un limite intrinseco della fattispecie.

L'evoluzione tecnologica, difatti, non ha apportato solo una modifica agli strumenti ma, con crescente frequenza, ha inciso sullo stesso contesto spazio-temporale in cui si svolge la prestazione lavorativa, alterandone profondamente la struttura. Il pensiero corre, ovviamente, al processo di digitalizzazione del lavoro e allo sviluppo subito dal lavoro a distanza (soprattutto in forma di lavoro "agile", o *smart working*): fenomeni da tempo osservati, ai quali la pandemia da Covid-19 ha impresso una drammatica accelerazione[53]. In un contesto nel quale la prestazione si svolge attraverso la connessione in rete, la (già di per sé incerta) nozione di "strumento di lavoro" perde

---

[50] ROCCHINI (2019), p. 154-155 (da cui è tratto il virgolettato).

[51] Cfr. Cass. civ. sez. lav., 27 maggio 2015, n. 10955, in *DeJure*. In letteratura, ROCCHINI (2019), p. 158; in termini critici, PINTO (2017), p. 135 ss.

[52] Sul punto insiste anche FLOR (2016), p. 176 ss., il quale considera problematica, da questo punto di vista, anche l'interferenza con il Codice *Privacy*, in virtù della quale i provvedimenti del Garante contribuiscono a definire cosa sia lo strumento di lavoro.

[53] In argomento, tra gli altri, BROLLO (2020), p. 553 ss.; con peculiare riferimento alle questioni relative al controllo a distanza nella fase emergenziale, SITZIA (2020), p. 495 ss. Prima della pandemia, v. l'istruttivo affresco di TULLINI (2017), p. 97 ss.

ogni presunta efficacia connotativa, nel senso che ogni strumento può convertirsi in forma di controllo, e altrettanto disagevole appare distinguere tra potere direttivo e potere di controllo del datore di lavoro. E la tendenza è destinata ad accentuarsi a causa degli sviluppi in tema di IA applicati al contesto lavorativo[54].

Sul piano penalistico ne risultano effetti poco preventivabili. Il datore è esposto al rischio di incorrere nella sanzione penale, tenendo conto che il reato previsto dall'art. 171 Codice *privacy* risulta già integrato dalla mera "installazione" dello strumento di controllo e che, trattandosi di contravvenzione, è imputabile anche a titolo di colpa. Il lavoratore può trovarsi esposto a strumenti riconducibili (ovvero a torto o a ragione ricondotti dal datore) al comma 2° dell'art. 4 St. Lav., il cui impiego produce dati, magari inutilizzabili ai fini del rapporto di lavoro (se non vi è stata un'adeguata informativa), ma acquisibili in sede penale (come si dirà).

Simili effetti derivano da un disallineamento della fattispecie penale dal substrato empirico per cui era stata concepita, al punto che la distinzione tra strumento prestazionale e strumento di controllo, più che incerta, rischia di divenire radicalmente indimostrabile, almeno in un processo penale. Nell'ottica di un complessivo ripensamento del rapporto di lavoro, sollecitato dal nuovo contesto tecnologico[55], sarebbe sì auspicabile continuare a garantire una ragionevole tutela al lavoratore – nei "luoghi" non fisici dove è eseguita la prestazione –, ma rimodulandone i connotati anche in vista delle esigenze di certezza del datore.

6. I controlli difensivi.

Ad un riequilibrio dei contrapposti interessi di datore e lavoratore ha storicamente mirato la categoria dei c.d. "controlli difensivi", elaborata dalla giurisprudenza, nel vigore della precedente disciplina, con riferimento a forme di controllo esercitate fuori dei limiti posti dall'art. 4 St. lav., ritenute nondimeno consentite in quanto volte a reprimere condotte illegittime dei lavoratori (principalmente costituite da reati contro il patrimonio, episodi di danneggiamento a beni aziendali, rivelazione di segreti aziendali). La dottrina non ha certo risparmiato critiche alla categoria in questione[56].

Con la riforma del 2015, che ha incluso la tutela del patrimonio aziendale tra le possibili esigenze alla base dell'autorizzazione, si è inoltre avuta l'impressione che la tematica dei controlli difensivi fosse stata superata dal nuovo dato normativo[57]. Del resto, il problema è in parte confluito in quello della definizione dello strumento di

[54] Rileva, a tal proposito, MAINARDI (2020), p. 357, che «[…] si assiste ad una subalternità del giurista al programmatore, quest'ultimo in grado di decidere il livello di garanzie da accordare ai lavoratori. Una linea di tendenza, peraltro, destinata ad acuirsi nel contesto della IA, se è vero che i comportamenti delle macchine "intelligenti" sono prevedibili solo in parte da chi ha creato gli algoritmi alla base del loro funzionamento».
[55] Cfr. MAINARDI (2020), p. 341 ss.
[56] In chiave retrospettiva, in luogo di molti, DEL PUNTA (2016), p. 85 ss.
[57] Si veda, ad esempio, ALVINO (2016), p. 18; DEL PUNTA (2016), p. 96-97; per un drastico ridimensionamento della categoria, anche DAGNINO (2015), p. 1000 ss.

lavoro ai sensi del comma 2 dell'art. 4 St. lav., dal momento che, ove ricorresse tale qualifica, ad esempio, per uno strumento telematico, non sussisterebbe il reato ed il dato registrato, o comunque reperito attraverso tale strumento, sarebbe tendenzialmente utilizzabile ai sensi del comma 3[58].

L'effettivo superamento della categoria resta però oggetto di dibattito dottrinale, né è un esito al quale pare rassegnarsi la giurisprudenza[59]. Alla luce della complessità della materia, in questa sede non possiamo che procedere a delinearne solo alcuni aspetti attinenti ad una trattazione di taglio penalistico[60].

6.1. Inquadramento nelle cause di giustificazione e utilizzabilità dei dati conseguiti attraverso il controllo.

Una volta che il datore abbia esercitato dei controlli vietati, pare difficile giustificare il suo comportamento in base alla successiva scoperta, tra i dati in tal modo acquisiti, di fatti illeciti dei dipendenti. Se la categoria è genericamente riferibile a queste ipotesi, sono dunque comprensibili i dubbi della dottrina giuslavoristica sulla sua tenuta logica e normativa. Né pare agevole distinguere tra controlli attinenti alla prestazione lavorativa e controlli aventi ad oggetto il solo illecito (che fuoriesce dalla prestazione), posto che, per rilevare l'illecito, di regola sarà stato necessario monitorare la complessiva attività del lavoratore[61].

La distinzione, semmai, diviene possibile solo quando il controllo sia stato indirizzato a far luce su concreti indizi emersi *aliunde* a carico dei dipendenti: in caso cioè di controlli da taluno definiti difensivi "in senso stretto"[62] o "*ex post*"[63] ovvero, secondo altri, esclusivamente volti all'accertamento di comportamenti penalmente rilevanti[64].

---

[58] FERRANTE (2020), p. 301.

[59] Tra le applicazioni più recenti, Cass. civ., sez. lav., 28 maggio 2018, n. 13266, in *DeJure*. In dottrina, per uno sguardo d'insieme, MARAZZA (2017), p. 27 ss.; CASSANO (2020), par. 4.

[60] In sede penale, per altro, l'espressione "controlli difensivi" pare avere un'accezione più ristretta, focalizzata alla sola necessità di accertamento dei reati. Lo evidenziava, nel vigore del vecchio art. 4 St. lav., TULLINI (2011), p. 90. Ma sul punto si insisterà nel prosieguo. Per una ricostruzione della giurisprudenza penale in tema di controlli difensivi, di cui segnala le oscillazioni, v. CURI (2017), p. 185 ss.

[61] Tali rilievi in MARESCA (2016), p. 524.

[62] V. ancora MARESCA (2016), pp. 525-526, per il quale la categoria comprenderebbe i «[…] controlli difensivi in senso stretto, mirati ad accertare selettivamente condotte illecite — anche di aggressione al patrimonio aziendale — di cui si presume, in base ad indizi concreti, siano autori singoli (o alcuni) dipendenti, anche se ciò avviene in occasione dello svolgimento della prestazione lavorativa. In questo caso si tratta di indagini che, salvo quelle condotte direttamente dalle autorità di polizia o dalla magistratura (il che esclude ovviamente l'applicazione dell'art. 4), possono essere attivate dal datore di lavoro avvalendosi di idonei strumenti tecnologici. Questi controlli si collocano al di fuori dell'ambito applicativo dell'art. 4, non avendo ad oggetto l'attività del lavoratore».

[63] COSCIA (2018), p. 871 ss.

[64] È la delimitazione dei controlli difensivi suggerita da MARAZZA (2017), p. 30 ss.

Viene qui in considerazione la tesi secondo cui i controlli difensivi sarebbero ineliminabili, quando persista un'esigenza di difesa del patrimonio aziendale non assecondabile mediante la procedura prevista dall'art. 4 St. lav., cioè ogniqualvolta i tempi per giungere ad un accordo o per ottenere l'autorizzazione siano palesemente inconciliabili con la tutela del patrimonio aziendale. In questo caso, si osserva, il comportamento del datore ricadrebbe nella legittima difesa nei rapporti tra privati, garantita dal combinato disposto degli artt. 2044 c.c. e 52 c.p., sempre che ne ricorrano i presupposti, individuati nella necessità di fronteggiare, mediante il controllo, un'aggressione ingiusta al patrimonio o alla persona, nell'impossibilità di adempiere "in tempo utile" le incombenze previste dall'art. 4, ed infine nella "proporzionalità tra lo strumento di difesa e l'offesa"[65].

Ci sembra che, anche ai fini della configurazione della responsabilità penale, siffatte esigenze non possano essere trascurate[66]. Vero è che i limiti posti dallo Statuto al potere di controllo del datore non possono essere rimessi in discussione da scriminanti tacite. Ma la fattispecie penale delineata dall'art. 4 St. lav. non si presenta *a priori* incompatibile con le cause di giustificazione comuni. Soltanto, la legittima difesa non sembra la scriminate più appropriata, almeno in relazione ai casi che di solito si prova a giustificare con il ricorso ai controlli difensivi.

In primo luogo, non è agevole appurare un pericolo attuale di offesa ingiusta: di norma, si avrà notizia di episodi già avvenuti, unita al timore, più o meno fondato, di subire altre offese; il che, almeno secondo la corrente lettura dell'art. 52 c.p.[67] (e salvo ricorrere ad ardite operazioni analogiche *in bonam partem*), ben difficilmente rivestirebbe il connotato della "attualità", ovvero dell'offesa in atto o imminente, ma comunque non meramente "prevedibile".

In secondo luogo, se resta ignota al lavoratore, l'attività di controllo non interferisce direttamente con la condotta illecita che si suppone egli stia realizzando, limitandosi semmai a documentarla; in altri termini, il controllo di per sé non possiede alcuna idoneità impeditiva di un pericolo imminente o attuale, nei termini riferiti dall'art. 52 c.p. alla reazione difensiva. Infine, una tale "reazione" potrebbe toccare anche soggetti diversi dall'offensore, avendo il controllo destinatari indeterminati o comunque non previamente limitabili agli autori dei fatti lesivi (ché anzi esso potrà essere volto proprio ad identificare questi ultimi): in questa parte, la condotta datoriale non potrebbe comunque essere giustificata dalla legittima difesa.

In realtà, se il controllo è indotto da esigenze di accertamento di illeciti (presumibilmente) già commessi – ovvero dalla necessità di svolgere "indagini"[68] –,

---

[65] È la tesi formulata da MAIO (2017), p. 68 ss. In senso adesivo, PROIA (2016), p. 572.

[66] Si pensi al caso di un datore che abbia fondati elementi per ritenere che un suo dipendente che stia trafugando segreti industriali o commerciali a proprio profitto (condotta riconducibile all'art. 623 c.p.), aggirando i mezzi di controllo concertati con le rappresentanze sindacali. Supponendo che un nuovo o diverso impiego di quei mezzi consenta di accertare l'illecito – a patto, ovviamente, di non essere svelato –, la scelta di violare l'art. 4 St. lav. non può essere *a priori* ingiustificabile.

[67] Ad esempio, con riferimento al caso dell'omicidio (preventivo) del marito "tiranno", Cass. pen., 21 giugno 2018, n. 48291, in *DeJure*.

[68] PROIA (2016), p. 573.

sembra più corretto valutarne le condizioni di legittimità alla luce dell'esercizio di un diritto (art. 51 c.p.), costituito, nel caso in specie, non tanto dal potere direttivo del datore (arginato proprio dall'art. 4 St. lav.), quanto dal diritto di difesa garantito dall'art. 24, comma 1 Cost. Si tratterebbe, con ciò, di trasporre in questa sede un principio che la giurisprudenza viene elaborando in un contesto affine, nel momento in cui sancisce l'operatività di questa causa di giustificazione rispetto a comportamenti antecedenti all'instaurazione di un giudizio, consistenti nella raccolta di dati di provenienza illecita, purché strumentali ad un successivo utilizzo processuale[69].

In questa chiave andrebbe riletto l'orientamento secondo cui «[…] sono utilizzabili nel processo penale, ancorché imputato sia il lavoratore subordinato, i risultati delle videoriprese effettuate con telecamere installate all'interno dei luoghi di lavoro ad opera del datore di lavoro per esercitare un controllo a beneficio del patrimonio aziendale messo a rischio da possibili comportamenti infedeli dei lavoratori, in quanto le norme dello Statuto dei lavoratori poste a presidio della loro riservatezza non fanno divieto dei cosiddetti controlli difensivi del patrimonio aziendale e non giustificano pertanto l'esistenza di un divieto probatorio»[70]. In realtà, non è il materiale ad essere utilizzabile in quanto derivante da un tipo di controllo (apoditticamente) ritenuto ammesso dallo statuto; piuttosto, è il controllo difensivo ad essere ammesso – o meglio: giustificato per il tramite dell'art. 51 c.p. –, se ed in quanto il materiale sia stato reperito allo scopo di essere utilizzato in un procedimento penale.

In altri termini, se si prende sul serio il nesso tra controllo difensivo e utilizzabilità dei suoi risultati, il carattere "difensivo" andrebbe appurato mediante uno scrutinio delle possibilità scriminati del diritto di difesa, incentrato sul bilanciamento tra diritto di difendere in sede penale il patrimonio aziendale e interessi perseguiti dall'art. 4 St. lav.; con la possibilità di sacrificare questi ultimi al primo, solo là dove il rispetto della procedura prescritta dalla disposizione statutaria minerebbe irrimediabilmente la tempestiva acquisizione dei necessari elementi probatori.

Entro siffatti termini, l'inquadramento dei controlli difensivi nell'art. 51 c.p. non equivarrebbe ad un'incondizionata legittimazione di ogni violazione dell'art. 4 St. lav.

È vero che, a differenza della legittima difesa, dalla struttura dell'esercizio di un diritto esula una valutazione in termini di stretta necessità del comportamento, dovendosi evincere i limiti della scriminante da un confronto tra la disposizione incriminatrice e quella attributiva del diritto[71]. Nondimeno, ogni controllo motivato

---

[69] Cfr. Cass. pen., sez. II, 25 novembre 2020, n. 2457, in *DeJure*: «Ciò che appare dirimente ai fini del riconoscimento della ricorrenza della scriminante è, dunque, la strumentalità e la proiezione finalistica della condotta rispetto all'esercizio del diritto da parte dell'agente con piena riconducibilità nell'area di operatività dell'art. 51 c.p. di tutte le estrinsecazioni del diritto di difesa, anche di quelle di natura anticipatoria, ove funzionalmente collegate alla tutela giudiziaria. A tanto consegue che s'appalesa del tutto legittima una lettura espansiva del diritto di difesa che abbracci tutte le modalità del suo esercizio non solo nel processo e nel procedimento, ma anche prima che gli stessi vengano instaurati». Nel caso in specie, la Corte ha ritenuto giustificato il fatto corrispondente al delitto di ricettazione di *files* di provenienza delittuosa.

[70] Cass. pen., sez. II, 30 novembre 2017, n. 4367, in *DeJure* (che richiama numerosi precedenti).

[71] Sui limiti generali di operatività della causa di giustificazione dell'esercizio di un diritto, LANZI (1983), p. 27 ROMANO (2004), p. 544 ss.; VIGANÒ (2021), pp. 857-858.

dalla mera finalità di prevenire un generico rischio di commissione di illeciti, non sorretto da elementi concreti, ovvero da presupposti di fatto dell'esercizio del diritto, o eccedente il limite della proporzionalità, cadrebbe fuori da ogni proiezione del diritto di difesa (o ne costituirebbe palese abuso)[72].

Per tanto, non sarebbero giustificati controlli continuativi o *ad explorandum*, attraverso l'installazione permanente di *software* aventi lo scopo proclamato di prevenire eventuali illeciti; tanto meno intrusioni nella vita privata del lavoratore ricadenti in specifiche e più gravi fattispecie di reato (ad esempio, in un accesso abusivo ad un sistema informatico col fine di ottenere informazioni sui presunti colpevoli)[73].

Ciò chiarito, i presupposti di fatto dell'esercizio del diritto vanno accertati con riguardo al momento della condotta. Cosicché, seppure il controllo (non autorizzato) non sia produttivo di alcun risultato utile alla causa del datore, esso potrebbe apparire legittimo in ragione di fondati indizi e dell'iniziale impossibilità di tutelare gli interessi aziendali attenendosi alla normativa statutaria. D'altro canto, l'errore sui presupposti di fatto della scriminante potrebbe ricadere nell'ipotesi disciplinata dall'art. 59, ult. comma c.p.[74].

Infine, non osta alla riconduzione dei controlli difensivi all'esercizio di un diritto – e quindi all'esclusione della responsabilità penale del datore per la presenza di questa causa di giustificazione – la previsione del comma 3 dell'art. 4 St. lav., che opera su un piano distinto, anche se connesso, dal precetto penale racchiuso nei primi due commi.

L'inutilizzabilità è espressamente riferita dal comma 3 "*a tutti i fini connessi al rapporto di lavoro*", e consegue ad un ulteriore (rispetto all'osservanza dei commi 1 e 2 dell'art. 4) e distinto inadempimento del datore, ossia al difetto di adeguata informazione sulle modalità d'uso dello strumento in conformità al Codice *privacy*[75]. A parte quanto si dirà sulla giurisprudenza europea relativa alla possibilità di prescindere da questo requisito (v. par. successivo), l'ingresso delle medesime informazioni in un procedimento penale – dall'acquisizione della *notitia criminis* all'eventuale ammissione in fasi successive – è retto da regole autonome.

Lo conferma la giurisprudenza della Cassazione penale, nel momento in cui sostiene l'utilizzabilità dei dati raccolti, a prescindere dal rispetto del regime statutario, sul presupposto per cui le garanzie procedurali previste dall'art. 4 St. lav. riguardino

---

[72] Per riprendere una formula giurisprudenziale, «è necessario, però, che l'attività posta in essere costituisca corretta estrinsecazione delle facoltà inerenti al diritto e non trasmodi in aggressioni della sfera giuridica altrui, che sia estranea al campo applicativo del diritto azionato» (così Cass. pen., sez. V, 29 ottobre 2014, n.52075, in *DeJure*).

[73] Sull'incompatibilità del reato previsto dall'art. 615-ter c.p., se realizzato ai danni della controparte processuale, con l'art. 51 c.p. (invocato in ragione del diritto di difesa), Cass. pen., sez. V, 29 ottobre 2014, n. 52075, cit.

[74] Ad esempio, il datore nutriva il sospetto, rivelatosi poi oggettivamente infondato, che in azienda avvenissero dei furti commessi dai dipendenti; ciò lo ha indotto ad agire violando l'art. 4 dello Statuto: se il sospetto è passato attraverso un vaglio negligente, residua una responsabilità colposa. In generale, sulla configurabilità di un errore sui presupposti di fatto dell'esercizio di un diritto, LANZI (1983), p. 43; sulla natura di limite oggettivo del c.d. fine dell'esercizio del diritto, *ibidem*, p. 33 ss.

[75] Cfr. DEL PUNTA (2016), p. 105.

soltanto rapporti di diritto privato e non possano avere rilievo nell'accertamento dei reati[76]. Tale orientamento è in linea con la generale tendenza a giudicare remissiva l'osservanza delle norme sulla *privacy* innanzi alle necessità di acquisizione di prove documentali nel processo penale (per esempio, di documenti visivi)[77].

Il punto meriterebbe di essere approfondito, esaminando i rapporti tra art. 4 St. lav. ed art. 190 c.p.p.: esame dal quale è giocoforza prescindere in questa sede [78]. Ci limitiamo a trarne la conferma di come la violazione del precetto contenuto nell'art. 4, comma 1 St. lav. possa essere astrattamente giustificata dal diritto di acquisire informazioni spendibili in sedi diverse da quelle precluse dal comma 3, ad esempio per denunciare un reato; precisando che, più che una generica necessità di accertare i reati (prerogativa dei pubblici poteri), dovrebbe essere il diritto di difesa a segnare il perimetro dell'inosservanza giustificabile. Ciò non toglie che la necessità di accertare i reati influisca in maniera determinante e, al tempo stesso, problematica sul nostro tema, come emerge anche dalla giurisprudenza della Corte EDU.

6.2. Le indicazioni della Corte Europea dei Diritti dell'Uomo: il fine legittimo di accertare reati e i nodi irrisolti del bilanciamento.

La Corte EDU si è occupata dei controlli a distanza in alcuni recenti arresti che, pur non riguardando il nostro ordinamento, hanno suscitato la viva attenzione della dottrina, proprio per le possibili ricadute sulla tematica interna dei controlli difensivi[79].

In particolare, nella decisione della Grande Camera, *Bărbulescu c. Romania*, del 5 settembre 2017 – relativa al controllo datoriale, finalizzato al licenziamento, di un *account* aziendale di messaggistica istantanea, utilizzato dal dipendente per fini privati –, muovendo dal presupposto che il controllo a distanza costituisce ingerenza nella vita privata del lavoratore, protetta dall'art. 8 CEDU, e che spetta allo Stato membro un obbligo positivo di tutela dalle ingerenze poste in essere dai privati, la Corte ha ribadito che nella concreta definizione di questo obbligo lo Stato gode di un margine di apprezzamento[80]. La discrezionalità dello Stato è però soggetta ad alcuni limiti, costituenti altrettante condizioni di legittimità del controllo a distanza: a cominciare dal fatto che il lavoratore debba essere «preventivamente informato della possibilità che il datore di lavoro controlli la corrispondenza e altre comunicazioni e dell'attuazione di tali misure»[81]. Nel caso in specie, la violazione di questo obbligo ha comportato un'infrazione dell'art. 8 CEDU[82].

---

[76] Così, Cass. pen., sez. II, 4 aprile 2019, n. 23172, in *DeJure*, in merito ai dati conseguiti tramite sistema GPS.
[77] In argomento, CAMON (2013), spec. pp. 135-136; BELVINI (2018), p. 797 ss.
[78] Spunti in TULLINI (2011), p. 86 ss.
[79] Si vedano, tra gli altri, CASTELLUCCI (2020), p. 138 ss.; FORMICI (2018), PERRONE (2018); SITZIA (2018), p. 506 ss.
[80] Corte EDU, Grande Camera, 5 settembre 2017, *Bărbulescu v. Romania,* Application n. 61496/08, spec. §§ 70-73; 111.
[81] *Ibidem*, § 121.
[82] *Ibidem*, §§ 133-141.

Le premesse da cui muove la sentenza *Bărbulescu* sono presenti in una altrettanto nota pronuncia della Grande Camera, *López Ribalda c. Spagna*, del 17 ottobre 2019, con riferimento alla videosorveglianza di alcuni cassieri di un supermercato spagnolo, autori di ammanchi sul luogo di lavoro[83]. A differenza del caso *Bărbulescu*, in *López Ribalda* il ricorso al controllo occulto si collega ad un sospetto di reati a carico dei dipendenti; ed il fine del controllo risiede proprio ed esclusivamente nella necessità di accertare tali illeciti.

Innanzi a tale circostanza, pur riproponendo il medesimo catalogo delle condizioni di legittimità del controllo fissate dalla sentenza *Bărbulescu*, la Corte è costretta ad attribuire un diverso peso al primo criterio, costituito dall'obbligo di informazione preventiva nei confronti del lavoratore[84]. Questo obbligo, difatti, non risultava adempiuto nel caso *López Ribalda*, nel quale il datore aveva installato alcune telecamere visibili ed altre nascoste, informando i lavoratori solo della presenza delle prime. Né poteva logicamente essere adempiuto, dovendo lo strumento per forza rimanere occulto, per conseguire la prova della condotta illecita. La Grande Camera (riformando il giudizio della Terza Sezione) non ha ravvisato alcuna violazione, alla luce di un contemperamento di questo presupposto con le altre condizioni di legittimità del controllo, la cui verifica, nel caso in specie, è chiamata a sopperire l'assenza di informazione preventiva[85].

In sostanza, nel caso in cui il controllo sia finalizzato all'accertamento di un illecito, i termini del bilanciamento tra interessi del datore e del lavoratore subiscono un consequenziale adattamento: cardine del bilanciamento è pur sempre la proporzionalità (alla cui stregua, tra l'altro, va valutata l'estensione spazio-temporale del controllo), ma il ragionevole sospetto della commissione di gravi illeciti assurge a fine legittimo del controllo occulto, se la prova dell'illecito non può essere conseguita altrimenti.

Il ragionamento è in linea con la definizione di un ambito penalistico di operatività dei controlli difensivi in chiave scriminante, proposta nel paragrafo che precede. Non sorprende che, dalla giurisprudenza europea, la Corte di cassazione abbia tratto, ultimamente, una conferma della legittimità dei controlli difensivi – quantomeno nell'accezione invalsa in sede penale –, riconducendo l'esegesi praticata sull'art. 4 St. lav. al criterio della proporzionalità affermato in ambito convenzionale[86].

Ferma la legittima sottoposizione dell'art. 4 St. lav. a tale lettura, ci si può chiedere, però, se nel nostro ordinamento i termini del relativo bilanciamento siano delineati con sufficiente chiarezza.

L'art. 8, comma 2 CEDU esige infatti che ogni ingerenza per un fine legittimo nel diritto al rispetto della vita privata sia prevista dalla legge. Nel nostro caso, i limiti operativi all'art. 4 St. lav. derivanti dai c.d. controlli difensivi – e, di conseguenza, le ingerenze nella vita privata del lavoratore derivanti dal ricorso a tale categoria – sono

---

[83] Corte EDU, Grande Camera, 17 ottobre 2019, *López Ribalda and Others v. Spain, Application n. 1874/13 and n. 8567/13*.

[84] Cfr. *ibidem*, §§ 116; 128; 131; 134.

[85] Cfr. CASTELLUCCI (2020), p. 141 ss.

[86] Cass. pen., sez. III, 14 dicembre 2020, n. 3255 cit.

frutto di elaborazione giurisprudenziale: la disposizione statutaria non fa espresso riferimento ad un esonero dall'autorizzazione sulla base della necessità di procedere all'accertamento di illeciti, tanto meno detta espliciti criteri di bilanciamento tra questa esigenza e gli opposti interessi dei lavoratori. Pur dovendosi ricordare che, in ambito convenzionale, il diritto giurisprudenziale è assimilato alla fonte legislativa, non è detto che il *case law* formatosi a livello interno soddisfi il requisito richiesto dall'art. CEDU.

Non spetta a chi scrive compiere questa verifica in ambito giuslavoristico, ma sul piano penalistico sarebbe auspicabile una definizione legislativa dei presupposti applicativi dell'istituto. E ciò non solo per ragioni sostanziali di determinatezza, ma anche per le ripercussioni sul diritto di difesa dei soggetti coinvolti.

Il punto è che il controllo volto all'accertamento di un illecito s'intreccia inevitabilmente con una finalità pubblicistica. Questa sfumatura è colta da un precedente della Corte EDU (richiamato da *López Ribalda*), nel quale la Corte aveva espressamente collocato, accanto all'esigenza di tutela del patrimonio aziendale, la necessità pubblicistica di "accertamento della verità", nell'ambito di un processo a carico dei presunti colpevoli, comprendente anche la dimostrazione dell'innocenza degli altri dipendenti[87]. È vero che la giurisprudenza della stessa Corte è costante nel rimettere al diritto nazionale la definizione degli effetti processuali derivanti da una violazione dell'art. 8 CEDU, limitando la sua verifica di compatibilità con l'art. 6 CEDU all'utilizzo di tali prove da parte delle autorità nazionali nel caso concreto. Ma proprio per questo parrebbe opportuna una esplicita presa di posizione del legislatore nazionale al riguardo.

La questione assume grande rilievo, nel momento i cui gli ordinamenti nazionali demandano ad un soggetto privato – al datore di lavoro come agli operatori economici in genere – compiti inerenti alla prevenzione e all'accertamento dei reati, istituzionalizzando, in un certo senso, quella finalità pubblicistica insita nel controllo sull'attività lavorativa volto ad accertare la commissione di un illecito[88]. Nel nostro ordinamento, si giunge così ad un fondamentale snodo sistematico: il rapporto tra divieto statutario di controlli a distanza e apparati di *compliance* diretti a prevenire il

---

[87] Così, testualmente, Corte EDU, V Sez., 5 ottobre 2010, *Köpke v. Germany,* application no. 420/07: «The Court further agrees with the labour courts' finding that the employer's interest in the protection of its property rights could only be effectively safeguarded if it could collect evidence in order to prove the applicant's criminal conduct in proceedings before the domestic courts and if it could keep the data collected until the final determination of the court proceedings brought by the applicant. This also served the public interest in the proper administration of justice by the domestic courts, which must be able to establish the truth as far as possible while respecting the Convention rights of all individuals concerned. Furthermore, the covert video surveillance of the applicant served to clear from suspicion other employees who were not guilty of any offence». La necessità di procedere all'accertamento di una condotta illecita è stata evocata anche nell'opinione dissenziente del Giudice Dodev alla prima sentenza sul caso *López Ribalda* (cfr. Corte EDU, Sez. III, 9 gennaio 2018, *López Ribalda and Others v. Spain*, Applications nos. 1874/13 and 8567/13, *Dissenting Opinion of Judge Dodev*: «[…] the conclusion of the majority contradicts the general principle of law: the applicants should not be legally allowed to profit form their own wrongdoing […]. Therefore, the Convention cannot be construed and interpreted in such a way as to allow wrongdoing».

[88] Dalla prospettiva dell'ordinamento tedesco, si veda EISELE (2012), p. 13 ss.

rischio di commissione dei reati, rappresentati soprattutto dai modelli organizzativi adottabili in base agli artt. 6 e 7 del d.lgs. 231/2001.

7. Responsabilità degli enti e controlli a distanza: considerazioni preliminari.

Il rapporto tra responsabilità da reato degli enti e controlli a distanza sull'attività lavorativa può essere analizzato da diverse prospettive. Premesso che non vi è un esplicito raccordo tra rispettivi testi normativi, va anzitutto rilevato che, non solo il reato previsto dall'art. 171, ma nessun altro reato previsto dal Codice *privacy* rientra tra i reati presupposto della responsabilità dell'ente ai sensi del d.lgs. 231/2001, nonostante la (sola) rubrica dell'art. 24-bis del decreto 231 faccia riferimento al trattamento illecito dei dati[89]. Ai sensi dell'ultima disposizione citata, l'ente potrà rispondere, solo se il controllo datoriale sfoci in uno dei reati contro la riservatezza ivi richiamati[90] (sempre se commesso nell'interesse o a vantaggio dell'ente).

Ciò detto, va comunque rilevato che la violazione dell'art. 4 St lav. può comportare l'applicazione di sanzioni amministrative nei confronti delle società da parte del Garante per la *privacy*, per via del richiamo operato dall'art. 114 Codice *Privacy*, che a sua volta costituisce norma nazionale di maggior tutela ai sensi dell'art. 88 GDPR sul trattamento dei dati nell'ambito dei rapporti di lavoro. Avvalendosi di tale strumento, il Garante è intervenuto nell'ambito dei servizi di consegna a domicilio tramite i c.d. "rider", gestiti mediante una piattaforma digitale ed altri strumenti relativi all'assistenza dei clienti, utilizzati (secondo il Garante) in modo difforme dal disposto dell'art. 4 St. lav. [91]. Il contenuto afflittivo di tali sanzioni può di fatto eguagliare quello delle sanzioni *ex* decreto 231, ma il meccanismo di ascrizione della responsabilità non passa attraverso i modelli organizzativi che, notoriamente, contraddistinguono il sistema delineato dal decreto 231.

Alla luce del fatto che l'ente può essere chiamato altrimenti a rispondere, più che la mancata inclusione dell'art. 171 Codice Privacy nel decreto 231, in questa sede preme evidenziare l'omessa considerazione, da parte del legislatore, delle complesse interazioni tra modelli organizzativi e adempimenti inerenti alla riservatezza del lavoratore. Nessun dubbio sul fatto che l'obbligo (o onere) di predisporre il modello organizzativo supponga il rispetto della normativa sulla *privacy* e dello Statuto dei lavoratori, ma, ad uno sguardo più attento, il rapporto tra siffatti adempimenti è percorso da una latente antinomia, sia nella fase antecedente che nella fase successiva alla commissione di un reato.

---

[89] La proposta di aprire la c.d. parte speciale del d.lgs. 231/2001 alla tutela della riservatezza del lavoratore è stata comunque avanzata dalla dottrina: v. CURI (2017), p. 191-192. In generale, sulle connessioni (irrisolte) tra normativa *privacy* e responsabilità dell'ente, FONDAROLI (2019), p. 206-207.

[90] Artt. 615-ter, 615-quater, 615-quinquies, 617-quater, 617-quinquies c.p., richiamati – insieme ad altri – dall'art. 24-bis d.lgs. 231/2001.

[91] Garante per la protezione dei dati personali, Ordinanza ingiunzione nei confronti di Deliveroo Italy s.r.l. - 22 luglio 2021, reperibile in: *www.garanteprivacy.it*.

7.1. Modelli organizzativi e compliance digitale.

I modelli organizzativi (e in generale gli adempimenti rientranti nel concetto di *compliance*) implicano sempre più spesso il ricorso a tecnologie di tipo informatico, come ad esempio l'uso di programmi in grado di processare i dati aziendali allo scopo di individuare anomalie, di tracciare le attività compiute dai dipendenti, al fine di evitare comportamenti elusivi o di ricostruire eventuali infrazioni, nonché di gestire i flussi informativi interni all'ente[92].

La *compliance* aziendale concorre dunque, con ogni evidenza, allo sviluppo di nuove tecnologie di controllo del lavoro. Il che accentua, in primo luogo, le difficoltà insite nella distinzione tra strumento di lavoro e strumento di controllo[93]. La parziale dipendenza della nozione di strumento di lavoro dal contesto organizzativo di volta in volta considerato suscita, anzi, un interrogativo di fondo, strettamente attinente alla *compliance*: l'impiego di uno strumento idoneo a monitorare l'attività del lavoratore, quale destinatario del modello organizzativo, può essere ricondotto *per ciò solo* al comma 2 dell'art. 4, cioè in quanto funzionale alla *compliance* aziendale? A tale interrogativo, a nostro avviso, va data risposta negativa[94].

Vero è che, in alcuni ambiti, mezzo prestazionale e misura di sicurezza tecnologica si compenetrano: si pensi alle misure dedicate alla prevenzione dei reati informatici, che richiedono l'applicazione di strumenti (*hardware* e *software*) volti a tracciare gli accessi e le modalità di utilizzo dei dispositivi aziendali da parte del lavoratore, oltre che finalizzati alla manutenzione della rete da parte dei responsabili IT[95]. In tal caso, la distinzione funzionale tra componenti del dispositivo finalizzate alla prestazione ed altre adibite ad un controllo sul lavoratore appare oltremodo complessa[96], per non dire impossibile.

Ma la questione è destinata a riproporsi, ogniqualvolta l'adozione di un presidio tecnologico sia ritenuta, allo stato delle conoscenze disponibili, la migliore o addirittura l'unica misura preventiva del rischio di inosservanza insito in una determinata attività lavorativa. Si pensi, ancora, al settore dell'anticorruzione, nel quale le tecniche di *compliance* spaziano dalla "rudimentale" registrazione dei colloqui tra esponenti aziendali e pubblici agenti, alle più sofisticate modalità predittive del rischio sulla base di *Big Data Analytics*[97].

---

[92] Per uno sguardo d'insieme, BIRRITTERI (2021), § 3; dal punto di vista giuslavoristico, MAINARDI (2014), p. 109 ss.

[93] *Supra*, §§ 5, 5.1., 5.2.

[94] La risposta trae supporto dalla lettura di MAINARDI (2014), p. 111.

[95] V. FONDAROLI (2019), p. 203, 207; GULLO (2021b), p. 389; diffusamente, VILLA E. (2014), p. 122 ss.

[96] Di «intricata ragnatela» parla VILLA E. (2014), p. 136-137, la quale muove comunque dalla premessa della necessità, da parte del datore, di adempiere gli obblighi previsti dall'art. 4 St. lav. (anche) per prevenire i reati informatici.

[97] Si vedano le prospettive delineate nel saggio di BIRRITTERI (2019), p. 289 ss.; con riferimento alla *compliance* ambientale, SABIA (2020), p. 193-194.

Più in generale, in un prossimo futuro, il complesso delle attività riconducibili alla *compliance* sarà sempre più gestito tramite tecnologie quali *Blockchain* ed intelligenza artificiale (AI)[98]. Il fenomeno, etichettato "*digital criminal compliance*", potrebbe comportare la sottoposizione dei dipendenti ad una capillare attività di controllo elettronico, i cui risultati potrebbero spingersi oltre la generica previsione di un rischio illecito in ambito aziendale, sino a tradursi in una vera e propria profilazione di lavoratori singoli o di gruppi, in base alla specifica attitudine a commettere infrazioni[99]. Si delineerebbe, con ciò, l'improprio affidamento al datore di lavoro di un'attività corrispondente all'accertamento della pericolosità criminale (su base tecnologica)[100]: scenario inquietante, che esigerebbe un più profondo ripensamento degli strumenti normativi a tutela del lavoratore.

In questa sede, ci si può limitare a constatare come, in mancanza di un espresso raccordo con la disciplina statutaria, da un lato, e di un vero e proprio "obbligo" di adottare i modelli organizzativi secondo contenuti legislativamente predefiniti[101], dall'altro, la mera inclusione di uno strumento di controllo in un *compliance program* non è di per sé sufficiente ad esimere il datore dagli obblighi sanciti dall'art. 4 comma 1 St. lav.; né potrebbe essere invocata la categoria dei controlli difensivi, incompatibile con la generica finalità di prevenire illeciti aziendali, per le ragioni a suo luogo illustrate.

Va anzi riconosciuto come l'adozione di un modello organizzativo attecchisca proprio nelle esigenze elencate dall'art. 4, comma 1 St. lav.: di tipo organizzativo, relative alla sicurezza del lavoro, nonché alla tutela del patrimonio aziendale (in quanto il modello consente all'ente di evitare in tutto o in parte le sanzioni a contenuto patrimoniale previste dal decreto 231). Da questo punto di vista, la riduzione del rischio reato rientra nei compiti organizzativi primari dell'organo di gestione, ottemperando ai quali è necessario che esso tenga in debita considerazione gli interessi dei lavoratori.

In sostanza, finché si consideri l'adozione del modello organizzativo *ante delictum*, l'eventuale allestimento di presidi tecnologici volti al monitoraggio dell'attività lavorativa non è sottratta alle rituali autorizzazioni.

7.2. Il nesso problematico con le indagini interne.

La prospettiva muta però, almeno in parte, se si guarda all'attività d'indagine successiva alla notizia di un'infrazione (non necessariamente tradottasi nella consumazione di un reato), qualora l'ente cominci ad indagare prima dell'avvio di un procedimento penale (in qualità di potenziale imputato o di persona offesa), come

---

[98] GULLO (2021a), p. 286 ss.

[99] Cfr. BURCHARD (2021), p. 741 ss.

[100] BURCHARD (2021), p. 747-748.

[101] Il dato rileva in quanto, per le attività che, invece, il datore debba obbligatoriamente porre in essere, si ritiene egli possa fare a meno delle autorizzazioni previste dall'art. 4: cfr. ZOLI (2016), p. 641, che fa l'esempio dei dischi cronotachigrafi degli autotrasportatori.

accade a seguito di una segnalazione interna *ex* art. 6, comma 2-*bis* d.lgs. 231/2001 (*whistleblowing*).

L'attività d'indagine interna all'ente non è organicamente regolata dalla legge, ma trova solo una frammentaria disciplina nell'ambito del d.lgs. 231/2001, che quantomeno la incentiva nelle parti relative alle c.d. condotte riparatorie dell'ente[102]. Allo stesso tempo, i risultati investigativi possono porre questioni di utilizzabilità o ammissibilità, anche in ragione dell'incerta riconducibilità ad una precisa categoria probatoria.

Pur al cospetto di un quadro normativo così sfuocato, non è escluso che l'impiego di uno strumento di controllo, privo di autorizzazione, possa ricadere nell'area dei controlli difensivi, trattandosi di attività strumentale all'esercizio della difesa dell'ente, che può ricavarne un'attenuazione o finanche l'esonero da responsabilità. Ma è appunto in tale frangente che il nostro ordinamento si rivela carente, non definendo chiaramente i limiti entro i quali l'ente può difendersi indagando.

Anzi: essendo incentivato a dimostrare che il reato è avvenuto nell'esclusivo interesse dell'autore persona fisica, e che quest'ultimo ha eluso fraudolentemente il modello organizzativo, l'ente è in una situazione di forte antagonismo rispetto alla posizione del dipendente sospettato di aver commesso il reato. Tanto che si è parlato di una mutazione del diritto di "difendersi provando" (spettante all'ente) in un diritto di "difendersi accusando" (il presunto autore del reato)[103]. In un simile contesto, il richiamo all'art. 51 c.p., nei termini esposti in precedenza[104], può avere esiti del tutto incerti, dato il carattere "aperto" della norma codicistica[105].

Auspicabile, dunque, un intervento legislativo volto colmare il vuoto normativo relativo alle indagini interne[106], che dovrebbe offrire l'occasione – tra le altre cose – per regolare organicamente il rapporto tra difesa dell'ente e diritti dei lavoratori. Siffatta regolazione dovrebbe mettere in conto che il riserbo è in una certa misura connaturato alle indagini interne, almeno nella fase iniziale, e dunque destinato ad entrare in rotta di collisione con la *discovery* sottesa all'art. 4 St. Lav. Senza al contempo trascurare che la possibilità (o la necessità) dell'ente-datore di lavoro di avvalersi dei più avanzati strumenti tecnologici a propria difesa incontra un limite nella dignità dei lavoratori coinvolti.

L'assetto normativo vigente lascia insoddisfatti entrambi i soggetti del rapporto.

Da un lato, l'organo che assume le vesti di datore di lavoro sottostà al rischio di violare il disposto dell'art. 4 St. lav., con le relative conseguenze penali, salvo confidare in un'incerta estensione dei controlli difensivi in chiave scriminante. Dall'altro lato, i lavoratori fruiscono di un'ambigua protezione processuale, in quanto l'inutilizzabilità degli elementi probatori ottenuti attraverso i controlli non autorizzati è circoscritta al

---

[102] Sui nessi tra disciplina del *whistleblowing*, condotte riparative e indagini interne, BARBIERI (2020), p. 197 ss. Sulle indagini difensive, si veda inoltre a MANCUSO (2020), p. 1255 ss.

[103] FLICK (2017), p. 3461, richiamato da BARBIERI (2020), p. 201.

[104] Spec. § 6.1. *supra*.

[105] Sull'assimilazione dell'art. 51 c.p. ad una norma penale in bianco, LANZI (1983), p. 7.

[106] Cfr. MANCUSO (2020), p. 1265 ss.

rapporto di lavoro. Gli stessi elementi potrebbero restare inutilizzati in un procedimento disciplinare attivato a seguito dell'infrazione del modello organizzativo, e nondimeno essere posti alla base dell'accusa (e di un'eventuale condanna) in sede penale. È chiaro, dunque, che qui non è solo in pericolo la *privacy* dei dipendenti, ma piuttosto il loro diritto di difendersi da prove documentali formatesi nel corso delle indagini interne, con relativi rischi di autoincriminazione[107]. Ed è al tempo stesso in discussione il contrapposto interesse dell'ente a dimostrare di aver attuato un sistema disciplinare "idoneo" ai sensi dell'art. 7, comma 4 lett. b), del decreto 231[108].

8. Rilievi conclusivi.

Se raffrontato alle ragioni che si reputano alla base della riforma avviata dal *Jobs Act*, dal punto di vista penalistico, l'intervento in materia di controlli a distanza si espone a più di un rilievo critico. In conseguenza della necessità di salvare l'art. 4 St lav. dalla «obsolescenza tecnologica della norma»[109], che ha prodotto un'inadeguata definizione degli strumenti di controllo, la fattispecie penale si scopre affetta da insuperabile indeterminatezza, non limata – anzi, per certi versi incrementata – dal persistente ricorso ai controlli difensivi.

Nelle pagine che precedono, si è suggerito un inquadramento (penalistico) di quest'ultima controversa figura nell'art. 51 c.p., come emanazione del diritto di difesa garantito dall'art. 24 Cost. Ma si è del tutto consapevoli della precarietà di una simile ricostruzione[110].

In particolare, i limiti di liceità delle condotte rientranti nella *compliance*, quali attività non solo concepibili in termini di esercizio di un "potere" direttivo del datore di lavoro, ma piuttosto come adempimento di un "obbligo" organizzativo[111], non possono essere affidati ai limiti scriminanti dell'esercizio di un diritto[112].

Nella prassi, il reato previsto dall'art. 171 Codice *Privacy* – nella parte connessa alla violazione dell'art. 4 St. lav. – è applicato soprattutto ai "tradizionali", anche se ancora diffusi, mezzi di controllo (tipicamente le videoriprese), ma appare difficilmente gestibile innanzi alle più sofisticate tecnologie. La funzione di fatto assolta dalla norma statutaria, a seguito della riforma, risiede più che altro nel regolare l'acquisizione di dati generalmente utilizzabili, là dove siano state osservate le norme a tutela della riservatezza[113]; al contempo, per il caso di inosservanza, l'inutilizzabilità è limitata all'ambito del rapporto di lavoro e non può essere trasposta *de plano* in sede penale.

---

[107] Su questi delicati profili connessi alle indagini interne, si rinvia ancora a MANCUSO (2020), p. 1259 s.
[108] Il punto è nitidamente colto da VILLA E. (2014), p. 137.
[109] DEL PUNTA (2016), p. 84.
[110] Comprensibili i dubbi espressi da GROTTO (2014), p. 66 (il quale, tuttavia, fa risalire il diritto scriminante agli artt. 2086 e 2104 c.c.).
[111] Un cenno in PROIA (2016), p. 555.
[112] Cfr. *supra*, § 7.1.
[113] Per approfondimenti, sul punto, si rinvia comunque alle riflessioni di TEBANO (2016), p. 349 ss., e di PROIA (2016), spec. p. 562 ss.

Da qui la necessità *de jure condendo* di correlare i presupposti dei controlli a distanza (anche) all'utilizzo in sede penale dei dati raccolti. Tale necessità potrebbe essere assecondata con l'espressa previsione di una specifica clausola di esonero da parte dello stesso art. 4 St. lav., nel contesto di una complessiva regolazione delle indagini interne, volta a focalizzare il momento del passaggio da un obbligo organizzativo al diritto di difesa dell'ente.

Bibliografia

ALVINO, Ilaria (2016): "I nuovi limiti al controllo a distanza dell'attività lavorativa dei lavoratori nell'intersezione fra le regole dello Statuto dei lavoratori e quello del Codice della *privacy*", *Labour Law Issues*, vol. 2, n. 1.

ARENA, Maurizio, CUI, Stefano (2012): *I reati sul lavoro. Sicurezza e igiene del lavoro, nuovo reato di "caporalato", tutela e libertà del lavoratore, risarcimenti* (Milano, Giuffré).

BARBIERI, Anna (2020): "*Whistleblowing* e *internal investigation*: una prospettiva di collaborazione dell'ente", *Sistema penale*, 6, pp. 197-208.

BELVINI, Lorenzo (2018): "Videoriprese non investigative e tutela della riservatezza", *Processo penale e giustizia*, 4, pp. 797-809.

BIRRITTERI, Emanuele (2019): "*Big Data Analytics* e *compliance*. Profili problematici delle attuali prassi applicative e scenari futuri", *Rivista trimestrale di diritto penale contemporaneo*, 2, 289-303

BIRRITTERI, Emanuele (2021): "Controllo a distanza del lavoratore e rischio penale", *www.sistemapenale.it.*

BROLLO, Marina (2020): "Smart o emergency work? Il lavoro agile al tempo della pandemia", *Il lavoro nella giurisprudenza,* pp. 553-570.

BURCHARD, Christoph: "Digital Criminal Compliance, in ENGELHART, Marc, KUDLICH, Hans, VOGEL, Benjamin (Editors), *Digitalisierung, Globalisierung und Risikoprävention, Festschrift für U. Sieber* (Berlin, Duncker & Humblot), vol. II, pp. 741-755.

CAIRO, Lorenzo, VILLA, Umberto (2019): "I controlli a distanza a quattro anni dal *Jobs Act*", *Il lavoro nella giurisprudenza*, 7, pp. 676-687.

CAMON, Alberto (2013): "Captazione di immagini (dir. proc. pen.)", in *Enciclopedia del diritto*, Annali VI (Milano, Giuffrè) pp. 133-149.

CARINCI, Maria Teresa (2016): "Il controllo a distanza dell'attività dei lavoratori dopo il "Jobs Act" (art. 23 D.Lgs. 151/2015): spunti per un dibattito", *Labour Law Issues*, vol. 2 No. 1.

CARINCI, Maria Teresa (2017): "Il controllo a distanza sull'adempimento della prestazione lavorativa", in TULLINI, Patrizia (editor), *Controlli a distanza e tutela dei dati personali del lavoratore* (Torino, Giappichelli), pp. 45-53 (numerazione delle pagine corrispondete all'edizione in formato Ebook).

CASSANO, Giulia (2020): "I controlli *ex* art. 4 l. n. 300/1970", *Il Lavoro nella giurisprudenza*, 7, pp. 778-784.

CASTELLUCCI, Sebastiano (2020): "I controlli difensivi nel bilanciamento della Corte Europea dei Diritti dell'Uomo", *Argomenti di diritto del lavoro*, pp. 138-148.

CONSULICH, Federico (2018): *Lo statuto penale delle scriminanti. Principio di legalità e cause di giustificazione: necessità e limiti* (Torino, Giappichelli).

COSCIA, Carola (2018): "Le modifiche all'art. 4 Stat. Lav.: dignità e riservatezza del lavoratore

continuano a prevalere sulla tutela del patrimonio aziendale", *Diritto penale e processo,* pp. 871-877.

CRISCUOLO, Claudia (2019): "Potere di controllo e computer aziendale", *Rivista italiana di diritto del lavoro,* II, pp. 9-15.

CURI, Francesca (2015): "A margine degli 'Appunti per uno studio sulla tutela e sulla rilevanza penale dello Statuto dei lavoratori'", in MANTOVANI ET AL. (Eds.), *Scritti in onore di Luigi Stortoni*, Bologna, BUP, 2015, p. 503-511.

CURI, Francesca (2017): "Profili penali dei controlli a distanza", in TULLINI, Patrizia (editor), *Controlli a distanza e tutela dei dati personali del lavoratore* (Torino, Giappichelli), pp. 181-195 (numerazione delle pagine corrispondente all'edizione in formato Ebook).

DAGNINO, Emanuele, "Tecnologie e controlli a distanza", *Diritto delle relazioni industriali*, 2015, pp. 988-1007.

DEL PUNTA, Riccardo (2016): "La nuova disciplina dei controlli a distanza sul lavoro (art. 23, D. Lgs. n. 151/2015)", *Rivista italiana di diritto del lavoro,* I, pp. 77-109.

EISELE, Jörg (2012): *Compliance und Datenschutzstrafrecht. Strafrechtliche Grenzen der Arbeitnehmerüberwachung* (Baden-Baden, Nomos)

FABOZZI, Raffaele (2020): "I controlli a distanza (di cinquant'anni)", *Massimario di giurisprudenza del lavoro*, 1, p. 59-94.

FERRANTE, Vincenzo (2020): "Potere di controllo e tutela dei lavoratori: riflessioni sparse sulle disposizioni dello "Statuto", alla luce delle più recenti modifiche", *Jus-Online*, 1, pp. 289-306

FLICK, Giovanni Maria (2017): "Giustizia penale ed economia pubblica e privata: profili problematici", *Cassazione penale,* pp. 3461-3471.

FLOR, Roberto (2016): "Diritto penale e controlli a distanza dei lavoratori dopo il c.d. *Jobs Act*", in LEVI, Alberto (editor), *Il nuovo art. 4 sui controlli a distanza. Lo Statuto dei Lavoratori dopo il* Jobs Act (Milano, Giuffré), pp. 161-179;

FONDAROLI, Désirée (2019): "La responsabilità di persone giuridiche ed enti per i reati informatici", in CADOPPI, Alberto, et al (Editors), *Cybercrime* (Milano, Wolters Kluwer), pp. 193-208.

FORMICI, Giulia (2018): "Lavoratori e tutela della privacy: l'evoluzione della giurisprudenza della Corte europea dei diritti dell'uomo, tra controllo della corrispondenza elettronica e videosorveglianza", *Osservatorio AIC.*

FURLOTTI, Paolo (2019): "Lo Statuto dei lavoratori e disposizioni penali", in CADOPPI, Alberto et al (eds.), *Diritto penale dell'economia*, Tomo I, 2ª edizione (Torino, Utet), pp. 1477-1510.

GROTTO, Marco (2014): "La rilevanza penale del controllo datoriale attraverso gli strumenti informativi", *Il Diritto dell'informazione e dell'informatica,*1, pp. 57-74.

GULLO, Antonio (2021a): "I modelli organizzativi", in LATTANZI, Giorgio, SEVERINO, Paola (eds), *Responsabilità da reato degli enti*, vol. I - *Diritto sostanziale* (Torino, Giappichelli), pp. 241-288.

GULLO, Antonio, "I reati informatici" (2021b), in LATTANZI, Giorgio, SEVERINO, Paola (eds), *Responsabilità da reato degli enti*, vol. I - *Diritto sostanziale* (Torino, Giappichelli), pp. 381-391.

INGRAO, Alessandra (2021): "Il controllo a distanza sulla prestazione dei ciclo fattorini tra *Scoober App* e GPS", *Labour & Law Issues*, vol. 7, n. 1, pp. R165-184)

LANZI, Alessio (1983): *La scriminante dell'art. 51 c.p. e le libertà costituzionali* (Milano, Giuffré).

MAINARDI, Sandro (2014): "Codici etici nella prevenzione dei reati di lavoratori e collaboratori, modello organizzativo e sistema disciplinare", in FONDAROLI, Désirée, ZOLI, Carlo (eds), *Modelli organizzativi ai sensi del D. lgs. n. 231/2001 e tutela della salute e della sicurezza nei luoghi di lavoro* (Torino, Giappichelli), pp. 107-121.

MAINARDI, Sandro (2020): "Rivoluzione digitale e diritto del lavoro", *Massimario di giurisprudenza del lavoro,* 2, 341-369.

MAIO, Valerio (2017), "Il regime delle autorizzazioni del potere di controllo del datore ed i rapporti con l'art. 8 della l. 148/2011", in TULLINI, Patrizia (editor), *Controlli a distanza e tutela dei dati personali del lavoratore* (Torino, Giappichelli), pp. 54-84 (numerazione delle pagine corrispondente all'edizione in formato Ebook).

MANCUSO, Enrico Maria (2020): "'Indagini interne' disposte dall'ente: sussidiarietà regolatoria e nuovi scenari cooperativi", in *Processo penale e giustizia,* 2, pp. 1254-1266.

MANNA, Adelmo, DI FLORIO Mattia (2019): "Riservatezza e diritto alla Privacy: in particolare, la responsabilità per omissionem dell'Internet Provider", in CADOPPI, Alberto et al (eds.), *Cybercrime* (Milano, Wolters Kluwer), pp. 892-940.

MARAZZA, Marco (2017): "I controlli a distanza del lavoratore di natura 'difensiva'", in TULLINI, Patrizia (editor), *Controlli a distanza e tutela dei dati personali del lavoratore* (Torino, Giappichelli), pp. 27-40 (numerazione delle pagine corrispondente all'edizione in formato Ebook).

MARESCA, Arturo (2016): "Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 dello Statuto dei lavoratori", *Rivista italiana di diritto del lavoro*, I, pp. 513-546;

NUZZO, Valeria (2018): "I 'softwares' che registrano la durata delle telefonate nei 'call center' sono strumenti di lavoro?", *Rivista italiana di diritto del lavoro*, II, pp. 307-316.

PADOVANI, Tullio (1985): "Il controllo a distanza dell'attività lavorativa svolta mediante elaboratori elettronici", *Rivista italiana di diritto del lavoro*, II, pp. 252-258.

PECORELLA, Claudia, DE PONTI, Riccardo (2011): "Impiego dell'elaboratore sul luogo di lavoro e tutela penale della *privacy*", *Dir. pen. cont.*

PERRONE, Francesco (2018): "Corte Europea dei Diritti dell'Uomo, sentenza López Ribalda c. Spagna: la tutela della privacy dopo Bărbulescu 2", *www.rivistalabor.it*

PINTO, Vito (2017): "I controlli difensivi del datore di lavoro sulle attività informatiche e telematiche del lavoratore", in TULLINI, Patrizia (editor), *Controlli a distanza e tutela dei dati personali del lavoratore* (Torino, Giappichelli), pp. 120-141 (numerazione delle pagine corrispondente all'edizione in formato Ebook).

PROIA, Giampiero (2016): "Trattamento dei dati personali, rapporto di lavoro e l'"impatto" della nuova disciplina dei controlli a distanza", *Rivista italiana di diritto del lavoro*, I, pp. 547-576.

ROCCHINI, Emilio (2019): "*Social network* e controlli a distanza. Alla ricerca di un difficile equilibrio, *Massimario di giurisprudenza del lavoro*, 1, p. 143-159

ROMAGNOLI, Umberto (1972): *Art. 4*, in *AA.VV., Statuto dei diritti dei lavoratori*, *Commentario del Codice civile*, a cura di A. Scialoja e G. Branca (Zanichelli, Bologna).

ROMANO, Mario (2004): *Commentario sistematico del Codice penale*, vol. I, 3ª ed. (Milano, Giuffré).

RUSSO, Marianna (2016): "*Quis custodiet ipsos custodes*? I "nuovi" limiti all'esercizio del potere di controllo a distanza", *Labour Law Issues,* 2016, vol. 2 n. 2.

SABIA, Rossella (2020): "Artificial Intelligence and Environmental Criminal Compliance", *Revue Internationale de Droit Pénal,* vol. 91, 1, pp. 179-201.

SEMINARA, Sergio (2020): *Codice penale e riserva di codice*, www.giustiziainsieme.it

SGUBBI, Filippo (1998): "Profili penalistici", *Rivista trimestrale di diritto e procedura civile,* pp. 753-763.

SITZIA, Andrea (2017): "Personal computer e controlli tecnologici del datore di lavoro nella giurisprudenza", *Argomenti di diritto del lavoro,* 3, pp. 804-838.

SITZIA, Andrea (2018): "Videosorveglianza occulta, privacy e diritto di proprietà: la Corte EDU torna sul criterio di bilanciamento", *Argomenti di diritto del lavoro,* 2, pp. 506-522.

SITZIA, Andrea (2020): "Coronavirus, controlli e "privacy" nel contesto del lavoro", in *Il lavoro nella giurisprudenza*, pp. 495-510.

STORTONI, Luigi (1974): "Appunti per uno studio sulla tutela e sulla rilevanza penale dello Statuto dei lavoratori", *Rivista trimestrale di diritto e procedura civile,* pp. 1419-1455.

TEBANO, Laura (2016): "La nuova disciplina dei controlli a distanza: quali ricadute sui controlli conoscitivi?", *Rivista italiana di diritto del lavoro*, I, pp. 345-368;

TULLINI, Patrizia (2011): "Videosorveglianza a scopi difensivi e utilizzo delle prove di reato commesso dal dipendente", *Rivista italiana di diritto del lavoro*, II, pp. 86-92.

TULLINI, Patrizia (2017): "Il controllo a distanza attraverso gli strumenti per rendere la prestazione lavorativa. Tecnologie di controllo e tecnologie di lavoro: una distinzione possibile?", in TULLINI, Patrizia (editor), *Controlli a distanza e tutela dei dati personali del lavoratore* (Torino, Giappichelli), pp. 85-107 (numerazione delle pagine corrispondente all'edizione in formato Ebook).

VIGANÒ, Francesco (2021): "Art. 51", in DOLCINI, Emilio, GATTA, Gian Luigi (eds), *Codice penale commentato*, fondato da E. Dolcini e G. Marinucci, 5ª ed. (Milano, Ipsoa), I, pp. 845-881.

VILLA, Ester (2014): "La prevenzione dei reati informatici: fra limiti al potere di controllo e tutela della *privacy* dei lavoratori", in FONDAROLI, Désirée, ZOLI, Carlo (editors), *Modelli organizzativi ai sensi del D. lgs. n. 231/2001 e tutela della salute e della sicurezza nei luoghi di lavoro* (Torino, Giappichelli), pp.122-137;

ZILIO GRANDI, Gaetano, PETTINELLI, Roberto (2020): "A cinquant'anni dallo Statuto. "'L'art. 4 è morto. Viva l'art. 4!'", *Lavoro Diritti Europa*, 2.

ZOLI, Carlo (2016): "Il controllo a distanza dell'attività dei lavoratori e la nuova struttura dell'art. 4, legge n. 300/1970", *Variazioni su temi di diritto del lavoro*, 4, pp. 635-650.