UNIVERSITÀ DEGLI STUDI DI PADOVA

DIPARTIMENTO DI SCIENZE POLITICHE, GIURIDICHE E STUDI INTERNAZIONALI

Corso di laurea *Triennale* in DIRITTO DELL'ECONOMIA

"IL POTERE DI CONTROLLO DEL DATORE DI LAVORO E LA TUTELA DELLA PRIVACY DEL LAVORATORE"

Relatore:
Prof.ssa FRANCESCA LIMENA

Laureando:
VERONICA VAROTTO
matricola N. 1233074

A.A. 2023/2024

INTRODUZIONE

Il diritto del lavoro, il quale si identifica come quel complesso di norme che regolano e disciplinano i rapporti di lavoro subordinato e che tutelano la libertà, i diritti personali e gli interessi economici del lavoratore, nonché la dignità dello stesso. La stessa Costituzione Italiana nel suo art. 1 cita "L'Italia è una Repubblica democratica, fondata sul lavoro", con questo indica che deve essere assicurato a ciascun cittadino la possibilità di avere un lavoro e che tutti i lavoratori devono essere messi nella condizione di riuscire a contribuire alla vita sociale, economica e politica del loro Paese.

Nel corso dei decenni si sono susseguite numerose riforme del lavoro; in questa tesi l'attenzione sarà rivolta alle conseguenze ricavabili all'interno dello Statuto dei Lavoratori scaturite in seguito all'entrata in vigore del Decreto Legislativo n. 23/2015, attuativo del cosiddetto "Jobs Act".

Verrà analizzato il contenuto degli articoli 2, 3 e 4 della legge n. 300/1970, con una particolare attenzione rivolta alle modifiche del suddetto articolo 4 in materia di "Impianti audiovisivi e altri strumenti di controllo", mettendo in evidenza le modifiche apportate dalla riforma del 2015.

Sarà, inoltre, chiarita, grazie a posizioni giurisprudenziali, la disciplina dei controlli che il datore di lavoro può eseguire nei confronti del suo personale dipendente, differenziando quelli che possono essere "controlli difensivi", da quelli che invece risultano essere veri e propri "controlli occulti".

Ci si occuperà del Decreto Legislativo 196/2003, Codice in materia di protezione dei dati personali: il focus sarà sugli articoli 113 e 114, inoltre verrà fatto riferimento anche all'articolo 88 del Regolamento UE 679/2016.

Nella definizione dell'ambito di applicazione di tale disciplina non mancheranno esempi pratici di strumenti di controllo in capo al datore di lavoro e di strumenti di lavoro a disposizione del lavoratore differenziando i casi in cui è lecito che il datore effettui un controllo, nel rispetto della privacy del lavoratore e della disciplina del Codice della privacy, nonchè del GDPR.

1. QUADRO NORMATIVO CHE DISCIPLINA IL RAPPORTO FRA CONTROLLO E PRIVACY

1.1 IL CONTENUTO DELL'ARTICOLO 4 DELLO STATUTO DEI LAVORATORI

L'articolo 4 dello Statuto dei Lavoratori è stato riformato dal cosiddetto "Jobs Act", attraverso l'articolo 23 del Decreto Legislativo n. 151/2015, in vigore dal 24 settembre 2015 ed ha introdotto consistenti novità nell'ambito delle possibilità del datore di lavoro di operare un controllo sull'attività lavorativa dei propri dipendenti.

Prima della riforma del "Jobs Act" vigeva il divieto assoluto di utilizzo di impianti audiovisivi e di altre apparecchiature tecnologiche che avessero la finalità di sorvegliare l'attività lavorativa: l'unica deroga a tale divieto era costituita dal previo accordo con le Organizzazioni Sindacali. Qualora il datore di lavoro avesse avuto la necessità di svolgere dei controlli sui lavoratori, per esigenze di produzione, di organizzazione, di sicurezza o per la tutela del patrimonio della propria impresa, avrebbe potuto installare le necessarie apparecchiature tecnologiche, esclusivamente previo accordo con i sindacati, oppure in mancanza di questi, attraverso l'autorizzazione del Ministero del Lavoro territorialmente competente.

Ad oggi la disciplina è sensibilmente cambiata, il nuovo articolo 4 ("Impianti audiovisivi e altri strumenti di controllo") al comma 1 non vieta più l'utilizzo dei controlli a distanza come prevedeva espressamente la versione in vigore fino al 2015, ma nonostante questo, mantiene un'impostazione volta comunque ad evitare un abuso od un uso non perfettamente conforme, consentendo il ricorso ad apparecchi tecnologici volti alla sorveglianza dell'attività lavorativa solo in caso di " esigenze organizzative, produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale"; inoltre è altresì necessario un "accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali". Nel caso, invece di unità produttive che dovessero essere ubicate in diverse province rispetto all'unità principale, o addirittura in regioni diverse, tale accordo potrà essere stipulato con le associazioni sindacali comparativamente più rappresentative sul piano nazionale; infine, in mancanza di questi

accordi sindacali, è possibile procedere con l'installazione di impianti e strumenti, previa autorizzazione della Direzione territoriale del lavoro.[1]

Il secondo comma della norma sancisce che le disposizioni del primo comma non verranno applicate nel caso in cui i dispositivi tecnologici venissero usati dal lavoratore durante la propria prestazione lavorativa e per gli strumenti di registrazione degli accessi e delle presenze.

Questo sta a significare che, nei casi appena citati, non si renderà necessaria alcun tipo di autorizzazione, né da parte delle associazioni sindacali, né da parte della Direzione territoriale del lavoro: viene legittimato una sorta di controllo diretto, che può essere effettuato senza vi siano ragioni produttive, organizzative o di sicurezza.

Infine il terzo comma prevede che le informazioni raccolte ai sensi dei commi primo e secondo, possano essere utilizzate a "tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal D.Lgs. n. 195/2003".

Fin da subito, sono stati segnalate alcune criticità applicative dell'articolo 4 dello Statuto dei Lavoratori, il comma secondo e terzo sono strettamente collegati, in quanto le tecnologie menzionate nel comma 2 sono sottoposte dal comma 3, "alla sola condizione dell'assolvimento da parte del datore di lavoro, di un obbligo di mera informazione adeguata ai lavoratori sulle modalità d'uso degli strumenti e di effettuazione dei controlli"[2]. Si può dedurre che il ruolo dei lavoratori e dei loro rappresentanti sia piuttosto passivo, in quanto sono semplicemente dei destinatari della comunicazione del datore, il quale, al contrario, dispone di un'ampia libertà circa la determinazione dei mezzi e dei modi di controllo: può determinare discrezionalmente come utilizzare gli strumenti tecnologici di lavoro ed i controlli eseguiti tramite gli stessi. Gli unici oneri in capo al datore sono la trasparenza informativa, ovvero il dovere di informare i lavoratori circa l'avvenimento dei controlli, attraverso una adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e, l'adoperabilità di essi esclusivamente per fini lavorativi.

---

[1] A. Del Ninno. *In vigore la riforma dell'art. 4 dello Statuto dei Lavoratori sui controlli a distanza: privacy dei lavoratori e nuove regole.* in www.diritto e giustizia.it. 2015.

[2] Bellavista Alessandro, Santucci Rosario. "*Tecnologie digitali, poteri datoriali e diritti dei lavoratori.*", in "*La sorveglianza digitale del datore di lavoro*" a cura di A. Trojsi. Giappichelli, 2022, pag 71 ss

Un altro aspetto dibattuto in merito al presente articolo riguarda quali siano gli "strumenti utilizzati dal lavoratore per rendere l'attività lavorativa", in quanto il legislatore non fornisce una definizione, ma li categorizza in modo piuttosto generico. Il tema verrà analizzato successivamente.

1.2 IL CONTENUTO DEGLI ARTICOLI 2 E 3 DELLO STATUTO DEI LAVORATORI

Fanno parte del quadro normativo che regola il controllo messo in atto dal datore di lavoro sull'attività lavorativa dei propri dipendenti anche gli articoli 2 e 3 della legge n. 300/1970, i quali si intitolano rispettivamente "Guardie giurate" e "Personale di vigilanza". In virtù di quanto predisposto da questi due articoli, il datore può avvalersi, in casi eccezionali, dell'intervento di determinate persone, anche diverse dalle guardie giurate, predisposte alla tutela del patrimonio aziendale e al controllo dell'adempimento delle prestazioni lavorative.

Secondo quanto disposto dall'articolo 2 il datore può impiegare la figura delle guardie giurate soltanto per scopi di tutela del patrimonio aziendale; questo sottintende il fatto che le suddette guardie non possano controllare l'attività lavorativa dei lavoratori: nei commi 2 e 3 viene specificato il contenuto del comma 1, precisando che le guardie giurate non possano accedere nei locali nei quali si svolge l'attività lavorativa, durante la stessa, se non per specifiche esigenze che attengono alla tutela del patrimonio aziendale (comma 3).

Il riferimento al patrimonio aziendale circoscrive il raggio di azione delle guardie giurate alla sola tutela dei beni appartenenti all'azienda, quali beni mobili, immobili e immateriali nella disponibilità del datore di lavoro; inoltre la limitazione di accesso ai locali in cui si svolge l'attività lavorative, fa dedurre che questa restrizione non venga applicata in locali aziendali in cui non si svolge attività lavorativa, quali, ad esempio, bagni, mense, spogliatoi e locali di svago del personale aziendale.

L'articolo 3 dello Statuto dei Lavoratori dispone che "i nominativi e le mansioni specifiche del personale addetto alla vigilanza devono essere comunicati ai lavoratori interessati".

Viene determinato il potere del datore di lavoro di ricorrere all'intervento di persone ancora diverse dalle guardie giurate, quali per esempio agenzie investigative, per la salvaguardia dei propri interessi e per la tutela del patrimonio aziendale, con il dovere in capo al datore di mettere a conoscenza i lavoratori che saranno oggetto di tali ispezioni, in merito al nome di chi svolgerà le suddette indagini ed in merito alle specifiche mansioni di tali soggetti.

Si deve sottolineare che tali agenzie investigative non dovranno sconfinare nel controllo vero e proprio dell'attività lavorativa (riservato al datore), ma dovranno attenersi ad operare nei modi consentiti dalla legge, limitandosi ad individuare condotte illegittime adottate dal lavoratore, qualora vi siano dei sospetti di illeciti in corso di esecuzione[3].

Questo articolo, letto in combinato con l'articolo 2, mira a bloccare le forme di controllo cosiddetto occulto, che potrebbe danneggiare i lavoratori, a favore del principio di trasparenza che deve essere mantenuto fra datore e lavoratore.

Ma cosa si intende per "controlli occulti"?

L'idea di base è di un controllo a cui viene sottoposto il lavoratore, ma del quale egli non possa essere a conoscenza. Secondo la Corte di Cassazione sono inammissibili i controlli difensivi occulti, cioè "quelli posti in essere dal datore di lavoro al fine di accertare comportamenti illeciti e lesivi del patrimonio aziendale, senza che i lavoratori interessati siano preventivamente informati del loro svolgimento e delle modalità con cui l'attività di sorveglianza sia svolta – solo laddove non riguardino in nessun caso né l'adempimento, né l'inadempimento dell'obbligazione contrattuale del lavoratore di prestare la propria opera, ma si limitino ad accertare gli atti illeciti del lavoratore" (Sentenza della Corte di Cassazione n. 10636 del 2 maggio del 2017)[4].

Rappresenta un esempio della posizione della giurisprudenza in merito ai controlli difensivi la Sentenza della Corte di Cassazione, sez. lavoro n. 19922/16.[5]

Tale sentenza enuncia che "I controlli difensivi sui dipendenti devono riguardare comportamenti specifici che esulano il rapporto di lavoro. Sono dunque legittimi solo quando riguardano specifiche condotte lesive estranee al rapporto di lavoro". Il caso riguardava la Corte d'Appello di Venezia che accoglieva solo parzialmente il reclamo

---

[3] *Il ruolo dell'agenzia investigativa nel controllo delle obbligazioni lavorative.* Di "La Redazione" www.dirittoegiustizia.it. 2018

[4] sentenza pubblicata in "IUS Lavoro" 24 ottobre 2017 (nota di: Apa Sabrina)

[5] sentenza pubblicata in "*Rivista Italiana di Diritto del Lavoro" 2017, 1, II, 26 (nota di: Criscuolo, Ingrao)*

proposto da una società (Fidelitas) contro una sentenza del tribunale di Padova, il quale aveva accolto l'opposizione di un dipendente di tale società in merito all'illegittimità del licenziamento intimato al lavoratore, per insussistenza dei fatti ed ordinava il reintegro nel posto di lavoro e l'accredito delle retribuzioni non percepite.

Al lavoratore veniva contestato di aver compilato un rapporto infedele rispetto al numero reale di ispezioni concluse durante il turno di lavoro, in quanto il veicolo che egli doveva utilizzare nello svolgimento della sua attività lavorativa si sarebbe trovato altrove negli orari indicati: risultava quindi che avesse effettuato un numero inferiore di ispezioni rispetto a quello riportato nel rapporto di servizio. Questa discrepanza tra quanto dichiarato nel resoconto e la posizione del veicolo, era stata rilevata dalla società Fidelitas tramite un sistema GPS satellitare installato all'interno dell'autovettura utilizzata dal lavoratore, motivo per il quale gli era stato intimato il licenziamento disciplinare per giusta causa.

Il Tribunale di Padova, in merito alla vicenda, aveva stabilito il reintegro del lavoratore nel posto di lavoro.

Successivamente, la società Fidelitas aveva fatto ricorso in Cassazione, adducendo una serie di motivazioni a sostegno del ricorso: secondo la società, infatti sussistevano tutti gli elementi per ritenere il controllo dell'autoveicolo tramite sistema di GPS, un "controllo difensivo", diretto, cioè all'accertamento che la condotta del dipendente fosse illecita e che la verifica fosse avvenuta solo in seguito a dei fondati sospetti, per questi motivi, sarebbe stata funzionale alla tutela del patrimonio aziendale.

Queste motivazioni sono state respinte dalla Corte di Cassazione in seguito all'accertamento che il sistema di GPS era stato installato previamente e senza nessun collegamento con la vicenda descritta, quindi prima che la società avesse potuto avere dei sospetti sull'operato del proprio dipendente. Nella decisione della Corte si evince la sussistenze dalla violazione dell'articolo 4 dello Statuto dei Lavoratori, da cui si deduce che il sistema di geolocalizzazione costituiva un vero e proprio controllo occulto, in quanto installato ben prima rispetto al periodo risalente all'epoca dei fatti e quindi prima che la società potesse nutrire dei sospetti fondati. Appare evidente che il controllo attraverso sistemi di GPS permetteva un controllo a distanza durante la prestazione lavorativa, non a tutela dei beni aziendali, inevitabilmente, quindi non era in gioco il patrimonio dell'azienda.

Dalla vicenda si evince che risulta illegittimo il licenziamento del lavoratore, il quale doveva essere reintegrato sulla base di tutte le prove addotte dalla società, basate sul sistema satellitare installato nell'autovettura.[6]

Soprattutto nell'età contemporanea, con l'implemento degli strumenti tecnologici, il controllo ha assunto nuove prospettive. Se fino a un decennio fa poteva essere costituito da una telecamera nascosta, o da una intercettazione telefonica, ad oggi può essere attuato con tecniche molto più "raffinate", ma che allo stesso tempo richiedono anche una notevole competenza informatica, è per questo che si rende fondamentale l'informativa fornita al lavoratore per metterlo a conoscenza delle modalità con le quali vengono eseguiti i controlli.[7]

La ratio con cui sono stati istituiti questi due articoli nel 1970 era di eliminare alcune prassi aziendali tipiche dell'epoca, impedendo che venissero condotte delle vere e proprie indagini di carattere poliziesco, riducendo, sulla base dell'articolo 2, l'attività delle guardie giurate, ad un'attività di carattere istituzionale che mira a tutelare il patrimonio dell'azienda e sulla base dell' articolo 3 si intende precludere la possibilità che il controllo avvenga in modo occulto e non conoscibile dai lavoratori.

E' ammesso un controllo realizzato tramite un'agenzia investigativa ingaggiata dal datore di lavoro al fine di accertare comportamenti illeciti al di fuori della normale attività lavorativa, anche se posti in essere nell'esercizio della stessa, in quanto non sono riconducibili all'ambito di applicazione delle norme statutarie. [8] L'eventuale intervento di un'agenzia investigativa può essere giustificato sia in ragione della commissione di illeciti astrattamente imputabili al lavoratore, sia in ragione di un mero sospetto che questi illeciti si stiano compiendo.

1.3 GLI ARTICOLI 113 E 114 DEL D.LGS 196/2003, CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

[6] *Corte di Cassazione, sez. Lavoro, sentenza n. 19922/16 in* www.dejure.it. 2016

[7] Ziccardi, Giovanni. *"Il controllo delle attività informatiche e telematiche del lavoratore: alcune considerazioni informatico giuridiche."* *Labour & Law Issues* 2.1 (2016): 57-58.

[8] Faleri, Claudia. *"Attività investigativa e accesso ai dati personali del lavoratore."* *Labour & Law Issues* 9.2 (2023): 25-27.

Nell'attuale contesto dell'era digitale è emersa la questione di proteggere tanto i diritti dei lavoratori, quanto i loro dati personali all'interno degli ambienti lavorativi. Le nuove tecnologie hanno rivoluzionato la raccolta, l'elaborazione e la conservazione dei dati, snellendo e semplificando le attività all'interno delle aziende, ma allo stesso tempo si è reso necessario un "occhio di riguardo" anche dal punto di vista giuridico per la tutela di tutte quelle informazioni appartenenti ai lavoratori, che sono oramai, di così facile reperimento.

In particolare è stato elaborato dall'Unione Europea il Regolamento generale sulla protezione dei dati (GDPR, *General Data Protection Regulation*), approvato con Regolamento UE 2016/679 del Parlamento e del Consiglio del 27 aprile 2016 e applicabile a partire dal 25 maggio 2018.

Fin dai primissimi articoli tale Regolamento si occupa di definire i principi-guida che devono fungere da fondamento a tutte le attività di trattamento dei dati personali: all'articolo 5 (Principi applicabili al trattamento dei dati), alla lettera a) enuncia il principio di "liceità, correttezza e trasparenza", per il quale i dati devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato; successivamente, alla lettera b) viene introdotto il principio di "limitazione delle finalità", con il quale si vuole circoscrivere il fine ultimo per cui i dati raccolti possono essere utilizzati, ovvero unicamente per finalità determinate, esplicite e legittime, per essere in seguito trattati con modalità compatibili con tali finalità. Alla lettera c) è enunciato il principio di "minimizzazione dei dati", ossia devono essere prelevati un numero minimo indispensabile per le finalità per le quali sono trattati; inoltre devono essere rispettati, il "principio di esattezza" enunciato alla lettera d), cos' come il "principio di limitazione alla conservazione", lettera e), il quale impone una conservazione dei dati in modo tale da permetterne l'identificazione degli interessati e per un periodo di tempo non superiore al conseguimento delle finalità per cui sono stati trattati; infine, tutti i dati raccolti devono essere trattati secondo il "principio di integrità e riservatezza", enunciato alla lettera f), per evitare che vengano trattati secondo modalità illecite o non autorizzate e che possono comportarne la perdita o la distruzione.

Il GDPR è in linea con la disciplina italiana dettata dal Codice in materia di protezione dei dati personali, conosciuto come Codice della privacy (D.Lgs. 196/2003), entrato in vigore nel 2004. Esso ha subito sostanziali modifiche a partire dal 2018, per adeguarlo

alla disciplina dell'Unione Europea, in seguito all'approvazione del GDPR avvenuta poco prima, con l'obiettivo di rafforzare ulteriormente la protezione delle persone fisiche in materia di trattamento dei dati personali.[9]

Per quanto riguarda le tematiche giuslavoristiche, risulta centrale il tema citato in precedenza del controllo a distanza dei lavoratori: per la correttezza del trattamento dei lavoratori di qualsivoglia azienda, è imprescindibile seguire simultaneamente sia la disciplina dello Statuto dei lavoratori, sia la disciplina del Codice della privacy.

Come ribadito in precedenza, la disciplina dei controlli a distanza, sancita dall' articolo 4 dello Statuto dei Lavoratori, stabilisce che tali controlli possano avvenire solo per motivazioni legate all'organizzazione del lavoro, alla produttività o alla sicurezza ed il lavoratore interessato deve essere informato circa l'esistenza di tale controllo.

E' strettamente necessario ribadire che il controllo a distanza deve essere proporzionato e deve rispettare la privacy dei lavoratori dell'azienda, infatti nell'eventualità in cui esso violasse i diritti dei lavoratori, questi possono fare ricorso all'Ispettorato territoriale del lavoro, oppure alle associazioni sindacali competenti, a tutela dei proprio interessi. Esiste un collegamento diretto tra l'articolo 114 del Codice della privacy e l'articolo 4 dello Statuto dei Lavoratori, così come tra l'articolo 113 del Codice e l'articolo 8 dello Statuto. L'articolo 113 del Codice rinvia all'articolo 8 dello Statuto dei Lavoratori: "Divieto di indagini sulle opinioni". Tale articolo 8 enuncia che "E' fatto divieto al datore di lavoro, ai fini dell'assunzione, come nel corso dello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore". L'articolo 113 del Codice della privacy, invece enuncia: "Resta fermo quanto disposto dall'articolo 8 della Legge 20 maggio 1970, n.300, nonché all'articolo 10 del decreto legislativo 10 settembre 2003, n. 276" (Riforma del lavoro Biagi).

Si noti che nel testo del presente articolo 113 è stato inoltre aggiunto un ulteriore riferimento, ossia all'articolo 10 del D.Lgs. 276/2003 ("Attuazione delle deleghe in materia di occupazione e mercato del lavoro, di cui la legge 14 febbraio 2003, n.30"), entrato in vigore appena pochi mesi dopo il Codice della privacy .

---

[9] Tortora, Adriano. "*Il nuovo regolamento europeo per la protezione dei dati (GDPR) e la figura del Data Protection Officer (DPO): incidenza sulla attività della pubblica amministrazione*." *Amministrativ@ mente-Rivista di ateneo dell'Università degli Studi di Roma "Foro Italico"* 5-6 (2018).

Il riferimento all'articolo 8 dello Statuto dei lavoratori vieta al datore di lavoro di effettuare delle indagini, anche per mezzo di terzi, sulle opinioni politiche, religiose e sindacali del lavoratore, nonché "su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore", "ai fini dell'assunzione" e "nello svolgimento del rapporto di lavoro".

Questa esigenza di tutela che si evince dai due articoli si estende anche alla fase anteriore all'assunzione del lavoratore, infatti nella valutazione del candidato, il datore può assumere tutti quei dati che provengono da colloqui di selezione, con annessi curriculum, che forniscono informazioni rilevanti ai fini della valutazione professionale del lavoratore; può inoltre assumere informazioni circa lo stato di salute, nel caso in cui il potenziale lavoratore dovesse essere adibito allo svolgimento di lavori pesanti o di lavori notturni[10].

Occorre ricordare anche l'articolo 6 della Legge 135/1990, il quale vieta di svolgere indagini volte ad accertare nei dipendenti o in possibili candidati, l'esistenza di uno stato di sieropositività.[11]

Riassumendo, quindi, il sistema delle due norme, quali l'articolo 8 dello Statuto e l'articolo 113 del Codice della privacy, mira a limitare l'acquisizione di informazioni appartenenti alla vita privata dell'individuo lavoratore, così come evita che pervengano al datore delle informazioni o delle notizie irrilevanti ai fini dell'esecuzione del contratto di lavoro tra le parti, perché in esso creerebbero delle patologie, che potrebbero anche essere oggetto di un trattamento più o meno sfavorevole nei confronti del lavoratore.

Fermo restando che l'acquisizione di dati personali non è in assoluto vietata, ma deve essere estremamente pertinente alla finalità di assunzione oppure allo svolgimento dell'attività lavorativa prevista dal contratto; stando alle disposizioni del GDPR, questi dati possono essere categorizzati come : dati anagrafici, sia del lavoratore che dei familiari stretti, nel caso in cui dovessero essere effettuate delle detrazioni fiscali per familiari a carico; i dati bancari, essenziali per l'erogazione della retribuzione; i dati biometrici che attestino lo stato di salute nel caso eventuale di uno status di malattia del lavoratore; i dati strettamente connessi all'attività lavorativa, come la tipologia di contratto, la qualifica

[10] F. Girolami *"Diritto alla privacy:protezione e regole per il trattamento dei dati personali del lavoratore nel settore privato"* Monotema n. 8/2017, pag 4

[11] R. Sciaudone "*Commentario al Codice della privacy*" Pacini Giuridica, 2023. in "*Raccolta di dati e pertinenza*" a cura di E. Pesaresi. pag 365

professionale, la retribuzione, l'orario di lavoro, eventuali provvedimenti disciplinari e l'andamento professionale in merito agli obiettivi prefissati.

L'articolo 10 del decreto legislativo 10 settembre 2003, n. 276 ha esteso il divieto del datore di lavoro di effettuare indagini sui lavoratori anche alle agenzie per il lavoro e agli altri soggetti pubblici o privati autorizzati o accreditati presso il Ministero del lavoro che operano nel settore delle politiche attive del lavoro. Suddetto articolo enuncia che è fatto divieto ai soggetti citati di "effettuare qualsivoglia indagine o comunque trattamento di dati ovvero di preselezioni di lavoratori, anche con il loro consenso, in base alle convinzioni personali, alla affiliazione sindacale o politica, al credo religioso, al sesso, all'orientamento sessuale, allo stato matrimoniale o di famiglia o di gravidanza, alla età, all'handicap, alla razza, all'origine etnica, al colore, alla ascendenza, all'origine nazionale, al gruppo linguistico, allo stato di salute nonchè ad eventuali controversie con i precedenti datori di lavoro, a meno che non si tratti di caratteristiche che incidono sulle modalità di svolgimento della attività lavorativa o che costituiscono un requisito essenziale e determinante ai fini dello svolgimento dell'attività lavorativa". Va evidenziato che nemmeno il consenso del lavoratore stesso potrà in alcun modo legittimare tali indagini.

Uno dei problemi a cui si è andati incontro negli ultimi anni, è costituito dal fatto che il confine fra vita privata e sfera lavorativa si fa sempre più sottile: di recente il Garante della privacy si è trovato ad affrontare casi riguardanti dispositivi mobili affidati ai lavoratori, dispositivi di geolocalizzazione GPS[12] (come citato in precedenza) installati in autoveicolo di proprietà aziendale oppure su smartphone, che hanno rimarcato il fatto che le tecnologie moderne consentono di tracciare i dipendenti in tutti i loro movimenti: nei luoghi di lavoro, nel tempo libero e nelle loro abitazioni, proprio grazie (o a causa) dei dispositivi mobili che al giorno d'oggi formano parte integrante degli effetti personali di ciascuno. Questi apparecchi possono dare il via ad un monitoraggio non giustificato ed abusivo, un'intrusione non autorizzata al di fuori dell'attività lavorativa.

Il Garante fa riferimento alle tecnologie "*mobile device management*"[13] , le quali consentono al datore di amministrare da remoto i *devices* di cui sono dotati i lavoratori interessati, anche nel caso essi svolgessero la propria attività lavorativa in modalità

[12] Provvedimento del Garante n. 1850581 del 4 ottobre 2011 e provvedimento n. 2471134 del 7 marzo 2013 in www.garantedellaprivacy.it

[13] R. Sciaudone "*Commentario al Codice della privacy*" in "*Raccolta di dati e pertinenza*" a cura di E. Pesaresi. Pacini Giuridica, 2023. pag 369

flessibile o da remoto, oppure, ancora, durante gli spostamenti per lavoro. Sono questi i casi, infatti, in cui potrebbe avvenire un monitoraggio indiscreto dell'attività al di fuori dell'ambiente fisico di lavoro, in un contesto privato.

Attraverso il provvedimento del 4 ottobre del 2011, n. 1850581, il Garante della privacy afferma che nel rispetto del principio di necessità, la posizione del veicolo di regola non dovrebbe essere monitorata continuativamente dal titolare del trattamento, ovvero dal datore di lavoro, ma solo quando ciò si renda necessario per il conseguimento delle finalità legittimamente perseguite.

Viene precisato che, partendo dal presupposto che i veicoli possono essere associati direttamente o indirettamente ai lavoratori, da cui vengono utilizzati, essi possono contenere anche informazioni personali ad essi riferibili e conseguentemente, al trattamento di tali informazioni si applica la disciplina contenuta nel Codice della Privacy. Pertanto, sulla base del principio di necessità e del principio di pertinenza e non eccedenza, ne consegue che i tempi di conservazione dei dati personali trattati, con riferimento ai dati di localizzazione, dovranno essere cancellati o resi anonimi una volta terminata la prestazione[14].

Un ulteriore tema di interesse per quanto riguarda la protezione dei dati del lavoratore, riguarda la cosiddetta "profilazione". All'interno delle aziende per quanto riguarda la selezione del personale, la tendenza ormai è di non basarsi solo ed esclusivamente sulle informazioni attinenti ai curricula ed ai colloqui di selezione, ma ci si sta spostando sempre di più verso "l'analisi automatizzata, anche mediante algoritmi, di informazioni personali molteplici e diversificate, elaborate in funzione predittiva, e dunque in termini di capacità, produttività e performance di un aspirante lavoratore."

Questo fenomeno prende il nome di "profilazione" attraverso la tecnica dei "*big data*" ed influisce notevolmente nell'ambito del processo di digitalizzazione dell'economia e del mercato del lavoro. Sono in costante aumento nuove tecniche denominate "*workforce*" o "*people analytics*", consistenti in programmi algoritmici mediante i quali vengono raccolti, analizzati ed elaborati dati, personali e non, appartenenti ai lavoratori, utili ad orientare il settore delle risorse umane all'interno di un'azienda, ad una scelta mirata e

[14] M. Soffientini "*Geolocalizzazione e impatto privacy*". Wolters Kluwer Italia s.r.l. 2017 pag 891

consapevole del ”miglior candidato possibile”, oppure all’elezione del miglior dipendente, o ancora, all’elezione del team di lavoro più funzionante.[15]

Le attività di profilazione sono contemplate espressamente dal GDPR, infatti all’articolo 22 vengono enunciate alcune garanzie circa il diritto di informazione e di opposizione degli interessati, in merito all’attività di profilazione, si legge infatti al comma 1 “**.** L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.” Per il Garante, tale articolo costituisce un divieto per il datore di prendere decisioni in modo totalmente automatizzato (decisione presa senza il coinvolgimento di un essere umano che influenzi o cambi il risultato attraverso la sua autorità o competenza[16]), anche per quanto riguarda la profilazione, nel caso in cui dovesse condurre ad un effetto legale o analogo sull’interessato.

L’ambito della profilazione si ricollega all’articolo 8 dello Statuto dei Lavoratori, con riguardo al divieto di indagini sulle opinioni.

Facciamo riferimento al Provvedimento del Garante della privacy n. 488 del 24 novembre 2016.[17]

Tramite questo provvedimento il Garante aveva considerato una piattaforma sul rating reputazionale di professionisti ed imprese, illecita. Tale piattaforma veniva gestita da un algoritmo, alla cui base sottostava un sistema di raccolta, verifica ed elaborazione dei dati personali, ai quali in una fase successiva venivano assegnati “indicatori alfanumerici in grado di misurare l’affidabilità reputazionale dei soggetti censiti”.[18]

L’illiceità di tale piattaforma era data dalle ripercussioni sulla reputazione dei soggetti, siano essi dipendenti, clienti o candidati, in quanto venivano prese in considerazione un numero eccessivo di informazioni riguardanti la vita professionale e la vita privata; sulla base di questa affermazione il Garante asserisce che occorre estrema cautela nell’affrontare tematiche simili, considerando che la reputazione che si vorrebbe misurare

---

[15] R. Sciaudone “*Commentario al Codice della privacy*” Pacini Giuridica, 2023. in “*Raccolta di dati e pertinenza*” a cura di E. Pesaresi. pag 370

[16] S. Borghi “*Decisioni automatizzate e profilazione: le indicazioni dei Garanti Europei*” www.privacy.it 2017

[17] Aimo, Mariapaola. *"Dalle schedature dei lavoratori alla profilazione tramite algoritmi: serve ancora l’art. 8 dello Statuto dei lavoratori?*". *Lavoro e diritto* 35.3-4 (2021): 593-596 e provvedimento del Garante della privacy n. 488 del 24 novembre del 2016, pubblicato in www.garantedellaprivacy.it

[18] Provvedimento del Garante n. 488 del 24 novembre del 2016. cit.

attraverso la piattaforma di Mevaluate, in quanto strettamente collegata alla considerazione delle persone stesse e della loro "proiezione sociale"[19], risulta connessa intimamente con la loro dignità, elemento che sta alla base, cardine della disciplina della protezione dei dati, di cui il Garante si fa portavoce.[20]

Un ulteriore provvedimento del Garante della privacy rientrante nella sfera di protezione dell'articolo 113 del Codice della privacy è il n. 302 del 21 luglio 2011 (doc. web. 1825852).

Era stato evidenziato che presso un ente pubblico economico, venivano distribuiti questionari di personalità tramite una società di selezione del personale, contenenti domande inerenti aspetti piuttosto intimi riguardanti la vita privata dei candidati. Tali domande spaziavano dalla sfera personale, ai precedenti giudiziari, chiedevano informazioni riguardo ai rapporti affettivi, con richieste molto specifiche sul grado di stabilità, alla vita sessuale, alle condizioni di salute psico-fisica del candidato, nonché in merito a interruzioni di gravidanza. o ancora in merito alle abitudini personali, quali fumo, al consumo di alcolici, o di droghe e in merito alle abitudini alimentari.

Tutte queste informazioni, una volta raccolte, venivano impiegate nell'ambito del processo di selezione dei candidati al fine di stimare "indici prognostici riferiti al rischio del soggetto di sviluppare, in presenza di determinate pressioni ambientali, disturbi e disadattamento nell'ambito familiare e socioprofessionale del soggetto"[21].

Il Garante ha rilevato la non congruità dei dati raccolti al fine dell'espletamento delle mansioni richieste ed ha dichiarato l'illiceità dei questionari presi in esame per violazione della disciplina dell'articolo 8 dello Statuto dei Lavoratori e dell'articolo 10 del D.Lgs. 276/2003. Si legge nella motivazione che l'intento del legislatore è di tutelare i candidati alla ricerca di un posto di lavoro "vietando espressamente ed, indipendentemente dal consenso dagli stessi eventualmente manifestato, la raccolta di alcune tipologie di informazioni individuate al fine di proteggere, oltre al diritto alla tutela della vita privata, la dignità della persona". Nel caso in esame la dignità della persona è oltraggiata a causa della richiesta di informazioni in merito alla sfera affettiva, sessuale, sanitaria, alle

---

[19] D. Bianchi *"Algoritmo reputazionale e consenso alla privacy. Basta una spiegazione nella lingua comune"*. www.dirittoegiustizia.it 2023

[20] F. Paolucci "*Consenso, intelligenza artificiale e privacy"* www.medialaws.eu 2021

[21] Provvedimento del Garante n. 302 del 21 luglio del 2011 in www.garantedellaprivacy.it

abitudini alimentari, e personali: informazioni assolutamente ed innegabilmente non necessarie ai fini della valutazione professionale.[22]

L'articolo 114 del Codice della privacy fa rinvio ai presupposti di liceità stabiliti dall'articolo 4 dello Statuto dei Lavoratori (Impianti audiovisivi e altri strumenti di controllo).

Per quanto riguarda l'opinione espressa dalla dottrina, si ritiene che sia venuto meno il divieto generale dell'utilizzo di impianti audiovisivi per finalità di controllo a distanza, e l'ambito dei controlli leciti è molto limitato, in quanto il controllo a distanza può avvenire soltanto per le finalità indicate dalla norma, mentre "si conferma la legittimità dei controlli a distanza esclusivamente finalizzati al controllo della prestazione lavorativa."

Lo stesso garante ha sottolineato la "sopravvivenza del divieto di controllo diretto sull'attività dei lavoratori", vietando egli stesso la raccolta sistematica delle comunicazioni elettroniche (mail) in transito sugli account aziendali dei lavoratori il divieto per il datore di lavoro di accedervi.[23]

L'ARTICOLO 88 DEL REGOLAMENTO UE 679/2016, REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI.

Tale articolo 88, intitolato "Trattamento dei dati nell'ambito dei rapporti di lavoro" stabilisce, al primo comma, che gli Stati membri dell' Unione Europea possono prevedere, tramite legge o tramite trattati, delle norme più specifiche per assicurare la protezione dei diritti e delle libertà riguardo al trattamento dei dati personali dei lavoratori dipendenti nell'ambito dei rapporti di lavoro, per finalità di assunzione, esecuzione del contratto di lavoro, compreso l'adempimento degli obblighi stabiliti dalla legge o da contratti collettivi, di gestione, pianificazione e organizzazione del lavoro, parità e diversità sul posto di lavoro, salute e sicurezza sul lavoro, protezione della proprietà del datore di lavoro o del cliente e ai fini dell'esercizio e del godimento, individuale o

[22] R. Sciaudone "*Commentario al Codice della privacy*" Pacini Giuridica, 2023 in "*Raccolta di dati e pertinenza*" a cura di E. Pesaresi. pag 376-377

[23] R. Sciaudone "*Commentario al Codice della privacy*" Pacini Giuridica, 2023. in "*Garanzie in materia di controllo a distanza*" a cura di M. De Bernart. pag 398-400

collettivo, dei diritti e dei vantaggi connessi al lavoro, nonché per finalità di cessazione del rapporto di lavoro.

Al secondo comma enuncia che "Tali norme includono misure appropriate e specifiche a salvaguardia della dignità umana, degli interessi legittimi e dei diritti fondamentali degli interessati, in particolare per quanto riguarda la trasparenza del trattamento, il trasferimento di dati personali nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune e i sistemi di monitoraggio sul posto di lavoro."

Nel contesto del GDPR, il principio di trasparenza enunciato al comma secondo impone che le informazioni destinate al pubblico siano facilmente accessibili e di facile comprensione e che sia utilizzato un linguaggio semplice e chiaro (si veda l'articolo 12 del GDPR "Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato").

La normativa europea del GDPR viene recepita in Italia con un decreto di adeguamento nel 2018, il Decreto Legislativo 101/2018 e vengono emanate delle linee guida al fine di garantire l'applicazione coerente delle norme sulla protezione dei dati personali (in linea con quanto stabilito dal GDPR) e allo stesso tempo un regime di protezione dei dati armonizzato per tutti i cittadini europei. Viene stabilito il principio fondamentale per cui ogni lavoratore, indipendentemente dal tipo di contratto a lui applicato, ha diritto al rispetto della vita privata, delle sue libertà e dignità; inoltre egli deve essere informato sufficientemente ed adeguatamente sulle modalità secondo le quali i suoi dati personali verranno trattati, in maniera chiara, semplice ed esaustiva e, nel caso dovessero essere previste delle forme di controllo del lavoratore, dovranno essere rispettate le norme nazionali (alla luce dell'articolo 4 dello Statuto dei Lavoratori).[24]

Il GDPR è ampiamente caratterizzato dal "*principio di accountability*": tale principio è stato istituito per responsabilizzare i titolari del trattamento dei dati personali, quindi i datori di lavoro, i quali dovranno sempre adottare dei comportamenti diligenti e tali da poter dimostrare la concreta adozione di misure messe in atto ai fini di assicurare l'applicazione del regolamento. Per dimostrare il rispetto degli obblighi di trattamento, il datore potrà aderire ad un codice di condotta o potrà usufruire di un meccanismo di

[24]P. Salazar "*Trattamento dati personali e rapporto di lavoro*: ecco com'è cambiata la disciplina" www.altalex.com 2018

certificazione, rilasciata da un soggetto accreditato così come stabilito dagli articoli 42 e 43 del GDPR. Grazie ad essa un'azienda può attestare il proprio livello di adesione alle indicazioni del GDPR in tema di protezione e trattamento dei dati personali. Tale certificazione è uno strumento utile per assicurare la trasparenza del trattamento ed incrementare un rapporto di fiducia tra datore e lavoratore, il quale potrà valutare il livello di protezione dei propri dati.[25]

2. APPLICAZIONE

2.1 GLI STRUMENTI DI LAVORO E GLI STRUMENTI DI CONTROLLO

Nel corso del tempo si è reso necessario valutare quali fossero i nuovi strumenti, figli dell'innovazione tecnologica, idonei a realizzare un controllo a distanza dell'attività dei lavoratori, che rientrassero nell'ambito di applicazione dell'articolo 4 dello Statuto dei Lavoratori. Deve essere, infatti, coordinata la necessità dell'azienda di usufruire delle nuove tecnologie nello svolgimento dell'attività d'impresa, con l'obbligo del datore di lavoro di proteggere la dignità e la riservatezza del lavoratore.

Uno dei limiti messi in luce dalla dottrina[26] con riguardo all'articolo 4 è rappresentato dal fatto che i nuovi strumenti tecnologici, siano essi strumenti di lavoro oppure no, posseggono la caratteristica intrinseca di ricostruire le fasi dell'attività lavorativa, tramite per esempio la connessione alla rete internet, nel caso di smartphone, pc o tablet, svolta dal lavoratore durante il suo orario e ne permettono l'accesso anche ai dati sensibili, ricavabili, per esempio, dalla cronologia dei siti internet visitati attraverso un computer, tali connessione e cronologia, infatti, permetteranno di avere un accesso ai siti consultati dal lavoratore; nonché consentiranno anche il potenziale accesso alla posta elettronica, così come permetteranno di mettere a conoscenza il datore di lavoro anche dei luoghi in cui il lavoratore si è recato, attraverso la localizzazione GPS di un'auto aziendale.

---

[25] Borrillo, Barbara. "*La tutela della privacy e le nuove tecnologie: il principio di accountability e le sanzioni inflitte dalle Autorità di controllo dell'Unione europea dopo l'entrata in vigore del GDP*R." *Diritti fondamentali* 2 (2020): 344-345.

[26] Alvino, Ilario. "*I nuovi limiti al controllo a distanza dell'attività dei lavoratori nell'intersezione fra le regole dello Statuto dei lavoratori e quelle del Codice della privacy*." *Labour & Law Issues* 2.1 (2016) pag. 7ss

Questo accesso ai dati sarebbe potenzialmente molto semplice ed a portata di mano del datore, quindi si rende necessario stabilire dei limiti per evitare che vengano estrapolate informazioni riguardanti all'attività lavorativa o la vita personale del lavoratore.

Come sostenuto dalla dottrina, il fatto che la disciplina dei controlli a distanza sia stata inserita nel Titolo I dello statuto, "libertà e dignità del lavoratore" sta ad indicare, "come il bene principalmente protetto dall'articolo 4 debba essere identificato nella dignità del lavoratore, da intendersi innanzitutto come diritto del lavoratore a svolgere la propria prestazione in un ambiente sereno, libero da condizionamenti che potrebbero derivare da qualunque forma di controllo occulto e continuativo"[27]. Allo stesso tempo però, se è vero che è diventato sempre maggiore il numero di interessi dei lavoratori che potrebbero essere lesi attraverso l'uso di apparecchiature tecnologiche, è altrettanto vero che l'implemento tecnologico e il conseguente impiego di strumentazione nelle imprese, potrebbe comportare per il datore di lavoro la necessità di dover far fronte a sempre crescenti esigenze di controllo, data la frequenza con cui le nuove tecnologie vengono impiegate nell'attività lavorativa

Va ricordato che ogni condotta datoriale in merito all'attività di controllo deve garantire al lavoratore un'adeguata informativa sulle modalità con cui verrà svolta e deve sempre essere garantito il rispetto delle disposizioni del Garante della privacy riguardanti la protezione dei dati personali; inoltre, come citato nel precedente capitolo è necessario il rispetto dei principi cardine, a mezzo dei quali deve essere svolto tale controllo, ovvero, secondo necessità, correttezza, trasparenza, pertinenza e non eccedenza.

Gli strumenti attraverso i quali il datore potrebbe attuare il controllo, ad oggi sono molteplici, riportando alcuni esempi: potrebbe installare programmi informatici che tengano un tracciamento (non puntale) della cronologia, in modo da verificare se il lavoratore, durante il suo orario di lavoro, si sia dedicato alla navigazione per svago, invece che allo svolgimento della sua prestazione lavorativa, o ancora, potrebbe installare programmi che consentano il monitoraggio della posta elettronica proveniente o destinata esclusivamente all'account aziendale assegnato al lavoratore.

[27] Alvino, Ilario. "*I nuovi limiti al controllo a distanza dell'attività dei lavoratori nell'intersezione fra le regole dello Statuto dei lavoratori e quelle del Codice della privacy*. cit

Per quanto riguarda gli strumenti di lavoro, prima della riforma del 2015, una parte della dottrina riteneva che essi dovessero essere considerati esclusi dalla disciplina dell'articolo 4 S.L., mentre, l'opinione in antitesi riteneva che anch'essi, così come gli strumenti di rilevazione degli accessi, potessero essere utilizzati solo previa autorizzazione delle Organizzazioni sindacali[28] o del Ministero del lavoro.

Per questo motivo, durante la vigenza del vecchio articolo 4, molte imprese ricorrevano all'installazione di strumenti di lavoro "non in regola", in quanto manchevoli dell'autorizzazione sindacale o ministeriale. Questo problema nasceva dal fatto che queste apparecchiature erano indispensabili ai fini dello svolgimento dell'attività lavorativa, motivo per cui, in alcuni casi le imprese preferivano operare senza autorizzazione, piuttosto che ricevere un diniego da parte del Ministero, od un'autorizzazione che sancisse dei limiti eccessivamente stringenti all'utilizzo delle apparecchiature. Alla luce di tali problemi applicativi, con la nuova formulazione dell'articolo 4 dello Statuto dei Lavoratori, il legislatore ha deciso di escludere l'autorizzazione per l'installazione degli strumenti di lavoro. Questa decisione snellisce decisamente il sistema da un punto di vista organizzativo delle imprese, considerando che l'uso di strumenti di lavoro tecnologici sono indispensabili nello svolgimento del lavoro e il lavoratore deve poterne disporre agevolmente: se l'articolo avesse mantenuto la sua originaria formulazione, un datore di lavoro si vedrebbe costretto a richiedere un'autorizzazione, anche solo per dotare i propri dipendenti di di un computer o di un indirizzo di posta elettronica.

La definizione di "strumenti di lavoro" escluso dall'onere di autorizzazione è ricavabile dal medesimo articolo 4, ai sensi del comma secondo: in primo luogo, tale strumento "deve essere utilizzato dal lavoratore", ovvero richiede una partecipazione attiva del soggetto nel suo utilizzo; in secondo luogo, tale strumento deve essere utilizzato "per rendere la prestazione lavorativa", cioè deve costituire il mezzo con cui il lavoratore esegue la sua mansione.

Rientrano nella categoria degli strumenti di lavoro il computer, lo smartphone, così come la posta elettronica e l'accesso a internet. Dibattuto è, invece, il tema se rientrino o meno

[28] Alvino, Ilario. "*I nuovi limiti al controllo a distanza dell'attività dei lavoratori nell'intersezione fra le regole dello Statuto dei lavoratori e quelle del Codice della privacy*." *Labour & Law Issues* 2.1 (2016) pag 23

in questa categoria gli strumenti tecnologici che siano incorporati nell'apparecchiatura utilizzata dal lavoratore: è il caso del sistema GPS.

Nel caso, per esempio, di un'azienda operante nella consegna di pacchi nel territorio, che si avvale di automezzi dotati di sistema di localizzazione GPS, esso è da considerarsi uno strumento di lavoro, poiché la sua esistenza ed il suo funzionamento sono essenziali allo svolgimento dell'attività lavorativa.

La questione sarebbe differente nel caso in cui il GPS fosse installato con lo scopo di prevenire e contrastare eventuali furti dell'autoveicolo: data questa circostanza rientrerebbe a soddisfare esigenze diverse dalla prestazione dell'attività lavorativa, infatti rientrerebbe nell'ambito di applicazione del comma primo dell'articolo 4 dello Statuto dei Lavoratori, in quanto rientrerebbe nella categoria degli strumenti di controllo[29]

I dispositivi che costituiscono gli strumenti di lavoro possono essere tanto di proprietà aziendale, quanto di proprietà del lavoratore: il fenomeno dell'utilizzo dei dispositivi di proprietà di quest'ultimo sia a scopo personale, che a scopo lavorativo prende il nome di "*bring your own device (BYOD)*". Poiché il dispositivo sarà usato dai dipendenti anche per scopi personali, il GDPR ha stilato alcune raccomandazioni indirizzate al datore di lavoro: egli, infatti non dovrebbe poter accedere alle sezioni del dispositivo, che si presume vengano utilizzate solo ed esclusivamente per scopi privati, come, per esempio, la galleria di immagini di uno smartphone. Un altro punto evidenziato è la necessità che il datore attui dei sistemi di trasferimento sicuro dei dati dal dispositivo del dipendente, alla propria rete in modo da consentire una distinzione tra l'uso privato e quello aziendale del dispositivo.[30]

2.2 GLI STRUMENTI DI REGISTRAZIONE DEGLI ACCESSI E DELLE PRESENZE

Così come la categoria degli strumenti di lavoro, anche gli "strumenti di registrazione degli accessi e delle presenze" non prevedono autorizzazione sindacale o ministeriale per

---

[29] Alvino, Ilario. "*I nuovi limiti al controllo a distanza dell'attività dei lavoratori nell'intersezione fra le regole dello Statuto dei lavoratori e quelle del Codice della privacy*." *Labour & Law Issues* 2.1 (2016) pag 23

[30] R. Sciaudone "*Commentario al Codice della privacy*" Pacini Giuridica, 2023. in *"Garanzie in materia di controllo a distanza*" a cura di M. De Bernart. pag 400

la loro installazione. Si attengono alla disciplina dell'articolo 4 comma secondo dello Statuto dei lavoratori sul piano giuslavoristico e alle disposizioni in materia di protezione dei dati personali[31]; mentre sul piano europeo ci si rifà alla sentenza della Corte di Giustizia C-55/18 del 14 maggio 2019[32], la quale ha sancito l'obbligo per tutti gli Stati Membri di prevedere un sistema di conteggio per stabilire in modo univoco ed oggettivo, il numero delle ore lavorate in regime ordinario e straordinario dal lavoratore. In tal modo, da un lato il dipendente avrà un quadro chiaro delle ore di lavoro svolte e dall'altro lato, il datore potrà controllare la puntualità e il rispetto degli orari lavorativi del personale. Nel caso di specie, avvenuto in Spagna, la Corte di Giustizia UE ha fornito chiarimenti in merito alla mancanza, all'interno di una banca, di un sistema di registrazione dell'orario di lavoro giornaliero svolto dai lavoratori impiegati dalla stessa. Un sindacato di lavoratori ha presentato dinanzi alla Corte spagnola un ricorso collettivo diretto contro la banca, chiedendo la pronuncia di una sentenza che dichiarasse l'obbligo, a carico di quest'ultima, di istituire un sistema di registrazione dell'orario di lavoro giornaliero svolto dai membri del suo personale, che consentisse di verificare il rispetto, degli orari di lavoro stabiliti l'obbligo di trasmettere ai rappresentanti sindacali le informazioni relative al lavoro straordinario effettuato mensilmente. La Corte di Giustizia dell'Unione Europea ha ritenuto che gli Stati membri debbano imporre ai datori di lavoro l'obbligo di predisporre un sistema oggettivo, affidabile e accessibile che consenta la misurazione della durata dell'orario di lavoro giornaliero svolto da ciascun lavoratore

Sono numerose le soluzioni a disposizione del datore di lavoro atte alla registrazione degli accessi e delle presenze in azienda dei dipendenti, si è passati dall'ormai obsoleto "cartellino" marcatempo, all'utilizzo di "*badge*", piuttosto che a dispositivi che utilizzano la geolocalizzazione, o la scansione dei dati biometrici attraverso il riconoscimento delle impronte digitali.

Andando con ordine, in merito ai sistemi che permettono la timbratura mediante geolocalizzazione, ci si riferisce all'uso di applicazioni installate sullo smartphone. Il Garante della privacy ha stabilito la necessità di fornire un'adeguata informativa ai dipendenti, garantendo tutti i diritti loro spettanti sulla base della normativa; inoltre dovranno essere effettuate nomine specifiche in merito a coloro che potranno trattare i

[31] Alvino, Ilario. "*I nuovi limiti al controllo a distanza dell'attività dei lavoratori nell'intersezione fra le regole dello Statuto dei lavoratori e quelle del Codice della privacy*." *Labour & Law Issues* 2.1 (2016): pag 20.
[32] sentenza in www.dejure.it

dati ottenuti dal sistema; il datore dovrà, poi adottare tutte le misure di sicurezza necessaria per preservare l'integrità dei dati raccolti e trattati.

L'applicazione attraverso la quale si effettuerà la timbratura per mezzo della localizzazione dovrà essere progettata in maniera tale da indicare nel dispositivo del dipendente che la localizzazione si trova in stato "attivo" attraverso un'apposita icona e non si potrà avere alcuna possibilità di accesso ad altri dati presenti nello smartphone dell'interessato. Infine una volta ottenuto il dato della geolocalizzazione del lavoratore, ai fini della rilevazione della presenza, esso deve essere cancellato.

In merito ai sistemi di rilevamento delle presenze che sfruttano dati biometrici, ci si riferisce alla scansione dell'impronta digitale, o al riconoscimento facciale o dell'iride.

Anche in questo caso si rende indispensabile la fornitura di un'informativa indirizzata ai lavoratori.

Per quanto riguarda la categoria dei lettori badge dotati di fotocamera, essi consentono di individuare l'accesso del dipendente tramite lo scatto di una foto ogni qualvolta egli si rechi in azienda all'inizio del proprio turno di lavoro.

Nonostante l'immagine della persona fisica non rientri nella categoria di dati particolari sancita dall'articolo 9 del GDPR, è da considerarsi ugualmente un dato personale. Suddetta categoria costituisce un tema piuttosto dibattuto a livello internazionale in quanto alcune giurisdizioni lo considerano un metodo di rilevazione delle presenze, alquanto invasivo: è il caso dell'Autorità Garante per la privacy francese, la quale ritiene che la modalità di scattare foto ai dipendenti sia in entrata, che in uscita sia troppo invasiva e non si attenga al rispetto dei principi di minimizzazione, necessità e proporzionalità sanciti dall'articolo 5 del GDPR.[33]

2.3 CASI IN CUI E' LECITO EFFETTUARE UN CONTROLLO DA PARTE DEL DATORE DI LAVORO

Come già ampiamente ribadito in precedenza, il rispetto della privacy del lavoratore è il principio cardine della legislazione italiana in materia di controlli messi in atto dal datore verso i suoi lavoratori dipendenti.

[33]L. Giannini, *"Sistemi di rilevazione delle presenze in azienda: guida pratica alla compliance"* www.agendadigitale.eu , 2023

La disciplina prevede che il datore, in accordo con le disposizioni sancite dagli articoli 2, 3 e 4 dello Statuto dei Lavoratori, possa installare un sistema di videosorveglianza, previo accordo sindacale o previa autorizzazione concessa dall'Ispettorato del lavoro; a seguito dell'installazione i dipendenti devono essere informati e dovranno essere apposte delle specifiche segnaletiche che informino il personale dipendente circa la posizione degli impianti di videosorveglianza, ben visibili nelle ore diurne, quanto nelle ore notturne. Se l'installazione di tali sistemi dovesse essere manchevole delle necessarie autorizzazioni, l'attività di controllo messa in atto dal datore risulterà illegale: sulla base di questo presupposto, di conseguenza, anche qualora fossero rilevate dalle telecamere attività dei dipendenti a scopi personali, o a danno dell'attività dell'impresa, non potrebbero essere usate le registrazioni per sanzionare il lavoratore coinvolto.

Questo controllo datoriale può esplicitarsi, oltre che attraverso l'impiego di telecamere o di guardie giurate (articolo 2 S.L.), anche attraverso apparecchi più sofisticati, come computer, reti internet e altri strumenti informatici.

Un esempio inerente alla tematica è espresso dalla sentenza della Cassazione Civile, sezione lavoro del 22 settembre 2021, n. 25732[34]. Secondo la vicenda, in seguito all'accertamento della diffusione di un virus nella rete aziendale, l'amministrazione del sistema informatico aveva eseguito l'accesso sul pc di una lavoratrice dopo aver notato che nella cartella "download" era presente un file scaricato da cui sarebbe partita la propagazione del virus in tutta la rete, e avrebbe criptato i file presenti all'interno dei vari dischi di rete aziendale, rendendo gli stessi illeggibili, quindi inutilizzabili.

In aggiunta erano stati rilevati sul pc della lavoratrice anche numerosi accessi da parte sua a siti extra lavorativi per un tempo prolungato, che mettevano in evidenza il fatto che la stessa avrebbe interrotto per un tempo significativo la sua prestazione lavorativa.

Per il Tribunale e la Corte d'Appello non vi era stata alcuna violazione dell'articolo 4 dello Statuto dei Lavoratori in capo al datore, essendo necessario il controllo del computer aziendale della lavoratrice al fine di individuare l'origine del virus che aveva coinvolto l'intera rete aziendale, per poter risolvere il problema e ripristinare l'efficienza di tutti i files.

---

[34] "Sospetto che dal pc aziendale del lavoratore sia partito un virus: lecito per il datore effettuare un controllo". di "La redazione" www.dirittoegiustizia.it e sentenza in www.bollettinoadapt.it 2021

La lavoratrice ricorre in Cassazione, che afferma il principio di diritto secondo il quale "sono consentiti i controlli, anche tecnologici, posti in essere dal datore di lavoro, finalizzati alla tutela dei beni, anche estranei al rapporto di lavoro, o ad evitare comportamenti illeciti, in presenza di un fondato sospetto circa la commissione di un illecito, purché sia assicurato un corretto bilanciamento fra le esigenze di protezione di interessi e beni aziendali, correlate alla libertà di iniziativa economica, rispetto alle imprescindibili tutele della dignità e della riservatezza del lavoratore, sempre che il controllo riguardi dati acquisiti successivamente all'insorgere del sospetto". Qualora non dovessero ricorrere queste condizioni, "la verifica dell'utilizzabilità dei dati raccolti dal datore di lavoro, dovrà essere condotta sulla base dell'articolo 4 dello Statuto dei Lavoratori considerando i commi secondo e terzo".

Sulla base di tale affermazione, la Corte di Cassazione accoglie il ricorso della lavoratrice.[35]

Quanto rilevato dalla Corte mette in luce il presupposto indispensabile della legittimità dei controlli difensivi, cioè sia la presenza di un sospetto fondato circa la commissione di un illecito da parte di un lavoratore sia che tale controllo venga eseguito soltanto successivamente all'insorgere del sospetto.

Se non esistesse questo legame cronologico fra sospetto e controllo, il datore di lavoro potrebbe indiscriminatamente raccogliere dati di qualsiasi genere e per un tempo indefinito, venendo meno, così, alle disposizioni dello Statuto dei lavoratori, nonché alla normativa in materia di privacy.

Questa decisione della Corte ha importanti implicazioni: innanzitutto, riconosce il diritto del datore di lavoro di esaminare l'attività informatica dei dipendenti in determinate circostanze, come nel caso di un potenziale attacco informatico proveniente da virus. Tuttavia, ciò non deve essere interpretato come un permesso incondizionato per il datore di lavoro di monitorare l'uso del computer dei dipendenti. Al contrario, tale monitoraggio è consentito solo se esiste un sospetto legittimo e fondato di attività illecita.

Inoltre, la sentenza ribadisce l'importanza dei diritti dei lavoratori e l'obbligo del datore di lavoro di rispettare tali diritti. Anche in presenza di sospetti, il controllo deve essere

[35] "*Sospetto che dal pc aziendale del lavoratore sia partito un virus*: lecito per il datore effettuare un controllo", a cura di "La Redazione". www.dirittoegiustizia.it 2021

esercitato in modo proporzionato e necessario, rispettando sempre la privacy e la dignità del lavoratore.

3. I REQUISITI DI LEGITTIMAZIONE

3.1 I REQUISITI DI LEGITTIMAZIONE PER IL TRATTAMENTO DEI DATI PERSONALI ALL'INTERNO DEL RAPPORTO DI LAVORO NEL RISPETTO DELLA PRIVACY

La definizione di "dato personale", la quale è contenuta all'interno dell'articolo 4 del Regolamento generale sulla protezione dei dati (GDPR), prevede che è considerato "dato personale", "qualsiasi informazione riguardante una persona fisica identificata o identificabile (ovvero l'interessato); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale."

La nozione del relativo "trattamento" è ricavabile dal medesimo articolo 4, in cui esso viene definito come qualsiasi operazione o insieme di operazione messe in atto, con oppure senza, l'ausilio di processi automatizzati, applicate ai dati personali raccolti: tale trattamento può essere quindi identificato nella registrazione, nell'organizzazione, nella strutturazione, nella conservazione, nell'adattamento o nella modifica, nell'estrazione, nella consultazione, nell'uso, nella comunicazione mediante trasmissione, nella diffusione o in qualsiasi altra forma di messa a disposizione; nonché nel raffronto o nell'interconnessione, nella limitazione, nella cancellazione o nella distruzione.

Sulla base di quanto sancito dal comma terzo dell'articolo 4 dello Statuto dei Lavoratori, il titolare del trattamento, ossia il datore di lavoro, può utilizzare le informazioni e i dati, solo se lecitamente raccolti tramite gli impianti audiovisivi e gli altri strumenti, regolati dai commi primo e secondo, per "tutti i fini connessi al rapporto di lavoro". Un ulteriore requisito di legittimazione al trattamento è costituito dall'obbligo di fornire al lavoratore un'adeguata informazione circa gli strumenti e le modalità con cui tali dati verranno raccolti: nel rispetto delle disposizioni delle disposizioni del Codice della privacy.

Il requisito della previa informazione del lavoratore costituisce un fattore di grande rilevanza, più volte ribadito dal Garante, in quanto sottolinea in modo deciso

l'incompatibilità con ogni forma di controllo occulto, come se dovesse rappresentare il "principale argine a un utilizzo pervasivo dei controlli sul lavoro".[36]
Il Garante individua i principi fondamentali da rispettare nell'applicazione del regime giuslavoristico, riguardo alla liceità del trattamento dei dati raccolti tramite impianti audiovisivi, o altri strumenti e la loro, conseguente, utilizzabilità. Tali principi sono individuati alla luce dell'articolo 4 del GDPR, già citato in precedenza.
Altro aspetto da non trascurare è il divieto, sancito dallo Statuto e richiamato dal Codice della privacy, di indagare in merito alle opinioni politiche, sindacali, o religiose del lavoratore, più in generale questo divieto si estende a tutti i fatti non rilevanti ai fini della valutazione dell'attitudine professionale.

Secondo la dottrina[37], il corollario normativo in materia di protezione dei dati, è costituito dall'articolo 88 del Regolamento UE 679/2016, insieme agli articoli 113, 114 e 171 (Violazione delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori) del Codice e agli articoli 4 e 8 dello Statuto dei Lavoratori.
Il combinato disposto di questa serie di articoli costituisce un corollario di garanzie che vanno a tutelare il lavoratore in maniera "rafforzata", essendo questo considerato appartenente ad una categoria "vulnerabile", ai sensi del Regolamento 679/2016, che menziona espressamente i "lavoratori dipendenti" tra le categorie di interessati vulnerabili.
Il sistema di garanzia assicurato da tali articoli, alla luce dell'articolo 117 del Codice della privacy, prevede che la violazione da parte del datore di lavoro degli articoli 4 e 8 dello Statuto, porti ad una sanzione amministrativa e penale.

Nella società moderna, il sempre maggiore utilizzo del web fa sì che la quantità di dati facilmente reperibili sia sensibilmente notevole e questo può costituire un rischio: nel caso di specie in cui l'utilizzatore di internet ed in particolare dei social network, sia un

[36] R. Sciaudone "*Commentario al Codice della privacy*" Pacini Giuridica, 2023. in *"Garanzie in materia di controllo a distanza*" a cura di M. De Bernart. pag 404

[37] R. Sciaudone "*Commentario al Codice della privacy*" Pacini Giuridica, 2023. in *"Garanzie in materia di controllo a distanza*" a cura di E. Pesaresi. pag 406

lavoratore subordinato od un aspirante tale, l'attenzione da porre, in merito ai dati immessi nel web, deve essere molta.

Come detto, la disciplina del Codice, quanto quella dello Statuto mirano a fornire una tutela al lavoratore contro tutti quei pregiudizi che potrebbero derivare da una acquisizione "sconsiderata" dei dati da parte del datore: egli infatti, dovrà venire a conoscenza dei soli dati rilevanti al fine dell'esecuzione della prestazione lavorativa. Si parla di "spersonalizzazione del rapporto"[38] quando sulla base dell'articolo 8 dello Statuto, si vuole evitare che vengano utilizzati dal lavoratore i dati rivelatori della personalità dell'interessato e, che questi vengano usati in modo "strumentale", tanto da creare una vera e propria patologia nel rapporto di lavoro stesso. In conclusione, tutte le informazioni, irrilevanti ai fini della valutazione professionale, indipendentemente dal fatto che siano segrete, riservate, oppure di dominio pubblico, non sono utilizzabili per incidere negativamente sul rapporto di lavoro

Ciononostante, si può concludere che la disciplina dell'articolo 113 del Codice della privacy e il relativo rinvio all'articolo 8 dello Statuto dei Lavoratori non vieti in assoluto l'acquisizione e l'impiego di dati sensibili da parte del lavoratore, ma la consenta unicamente ai fini della gestione del rapporto.

3.2 IL GARANTE DELLA PRIVACY E IL MONITORAGGIO DI EMAIL E INTERNET NEI LUOGHI DI LAVORO

Tramite il provvedimento numero 1387978 del 5 marzo del 2007, il Garante della privacy stabilisce le linee guida per la posta elettronica e internet nell'ambito del rapporto di lavoro.

Stabilisce che i datori di lavoro, siano essi pubblici o privati, non possono controllare la posta elettronica, né la navigazione internet dei propri dipendenti, salvo in casi eccezionali. Spetta, inoltre al datore di lavoro la definizione delle modalità d'uso di tali strumenti, sempre tenendo in considerazione i diritti dei lavoratori e la disciplina in tema di relazioni sindacali.

[38] Iaquinta, Francesca, and Alessandra Ingrao. *"La privacy e i dati sensibili del lavoratore legati all'utilizzo di social networks. Quando prevenire è meglio che curare."* *rel. ind* (2014). pag 19

Il Garante prescrive ai datori l'obbligo di dare un'informazione chiara ai lavoratori, sulle modalità di utilizzo di internet e della posta elettronica e relative modalità con cui possono essere effettuati i controlli; ciò che invece vieta, è la "lettura" e la "registrazione sistematica delle email", così come il "monitoraggio sistematico delle pagine web visualizzate dal lavoratore", infatti tali due attività costituirebbero un vero e proprio controllo a distanza, nel caso in cui non sussistessero i requisiti necessari.[39]

Anche successivamente, con il provvedimento numero 53 del 2018 doc. web. num. 8159221, il Garante ha voluto confermare la sua posizione in merito, in cui ribadisce il divieto di "controllo massivo" e la conservazione illimitata delle email aziendali.

La giurisprudenza ritiene che l'accesso alle email dei dipendenti da parte del datore, in un account aziendale, possa considerarsi legittimo se correlato al fine di accertare o meno il potenziale comportamento lesivo dell'immagine dell'azienda o del patrimonio aziendale. Infatti, riallacciandoci alla disciplina dello Statuto, secondo la quale non è più necessaria l'autorizzazione sindacale per l'utilizzo degli strumenti di lavoro, anche per le informazioni che derivino da questi c'è la possibilità che vengano utilizzate per tutti i fini connessi al rapporto di lavoro, sempre a condizione che ne venga data informazione al lavoratore.

Il divieto, fatto al datore dal Garante, è di "controllo massivo" e di "conservazione illimitata delle email aziendali".

Il Provvedimento più recente adottato dal Garante, specifico in materia di trattamento dei dati personali all'interno di un contesto lavorativo, tramite programmi e servizi informatici di gestione della posta elettronica, quindi delle email, risale al 21 dicembre del 2023. Il documento di riferimento si intitola "Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati" (num. 9978728).

Si intendono "metadati" i dati esterni delle email, quali giorno, ora, mittente, destinatario, oggetto e dimensione degli allegati, di conseguenza non sono compresi i contenuti.

Lo stesso Garante si era già occupato del tema con un provvedimento del 1 dicembre del 2022 (num. 9833530), il cui oggetto principale consisteva nella "generalizzata raccolta e prolungata conservazione dei metadati relativi all'utilizzo della posta elettronica da parte

[39] *"Lavoro: le linee guida del Garante per posta elettronica e internet"* 5 marzo 2007 [1387978] www.garantedellaprivacy.it

dei dipendenti, per generiche finalità di sicurezza informatica". E' stato precisato che la raccolta e l'estesa conservazione dei metadati della posta elettronica non sono strumentali allo svolgimento della prestazione lavorativa del dipendente ai sensi dell'articolo 4 comma secondo dello Statuto, ma rientrerebbero piuttosto nell'ambito del comma primo.[40] Attraverso tale provvedimento è stato chiarito che i metadati relativi alla posta elettronica dei lavoratori dipendenti, una volta raccolti, possono essere conservati per un lasso di tempo massimo di sette giorni, estendibili, in presenza di comprovate esigenze che ne giustifichino il prolungamento, di altre quarantotto ore.

Possiamo dire che la tematica dell'utilizzo della posta elettronica sul luogo di lavoro coinvolge molteplici livelli di disciplina nel nostro ordinamento, rilevanti sono quelli del diritto penale che puniscono chi violi la privacy della corrispondenza di soggetti terzi. La corrispondenza elettronica risulta chiusa per coloro i quali non sono legittimati all'accesso al sistema informatico o alla ricezione dei messaggi; per "corrispondenza chiusa" si fa riferimento ad uno scambio di messaggi all'interno di un sistema protetto da una password: secondo la dottrina è lapalissiano che i colleghi all'interno di un ambiente lavorativo non siano autorizzati a violare questa chiusura della corrispondenza personale di qualcun altro protetta da una password, ma ci sono dei dubbi per quanto riguarda il datore di lavoro, in quanto proprietario del dispositivo informatico, ad esempio un computer, o del sistema di connessione. Per far luce sulla questione è utile distinguere tra chi è titolare del sistema che permette l'invio o la ricezione del messaggio e chi è, invece, titolare della conoscibilità del messaggio trasmesso. Come disciplinato dalle direttive n.46/95 e n.58/2002 CE il controllo della posta elettronica ed il relativo trattamento di dati personali è sottoposto alla disciplina della riservatezza: per tale motivazione appare chiaro che le informazioni sul lavoratore, riconoscibili in relazione all'esecuzione della prestazione lavorativa, comprese quelle ricavabili dalla corrispondenza elettronica rientrano nell'ambito applicativo del principio di riservatezza trattato dalle suddette direttive della CE, anche se la corrispondenza, quindi lo scambio di mail in questione sia

[40] R. Sciaudone "*Commentario al Codice della privacy*" Pacini Giuridica, 2023. in *"Garanzie in materia di controllo a distanza*" a cura di E. Pesaresi. pag 409

avvenuto in piattaforme (hardware) di proprietà dell'azienda, messe a disposizione del lavoratore nell'esercizio della sua attività lavorativa.[41]

Ci sono altre teorie secondo cui il mero fatto per cui le email siano ricevute nella casella di posta aziendale denoti che siano indirizzate direttamente all'impresa e pertanto il lavoratore, per mezzo dell'utilizzo della casella di posta aziendale accetti automaticamente il rischio che il datore potrebbe sempre accedere liberamente ai messaggi in entrata o in uscita, in quanto proprietario del computer.

In ambo i casi, è innegabile che, all'interno di un'azienda, se la posta elettronica fosse facilmente accessibile a tutti, compreso al datore di lavoro, ci sarebbe più di un aspetto problematico, per questo l'appartenenza della casella postale all'azienda, o del sistema informatico al datore, non implicano che tutti i messaggi che vi transitano siano automaticamente di pertinenza dell'azienda.

Come già detto, la disciplina sulla tutela della privacy non esclude del tutto la possibilità del datore di accedere alla casella di posta del lavoratore, né di ricezione dei messaggi; per "corrispondenza chiusa" si fa riferimento ad uno scambio di messaggi all'interno di un sistema protetto da una password: secondo la dottrina è lapalissiano che i colleghi all'interno di un ambiente lavorativo non siano autorizzati a violare questa chiusura della corrispondenza personale di qualcun altro protetta da una password, ma ci sono dei dubbi per quanto riguarda il datore di lavoro, in quanto proprietario del dispositivo informatico, ad esempio un computer, o del sistema di connessione. Per far luce sulla questione è utile distinguere tra chi è titolare del sistema che permette l'invio o la ricezione del messaggio e chi è, invece, titolare della conoscibilità del messaggio trasmesso. Come disciplinato dalle direttive n.46/95 e n.58/2002 CE il controllo della posta elettronica ed il relativo trattamento di dati personali sono sottoposti alla disciplina della riservatezza: per tale motivazione appare chiaro che le informazioni sul lavoratore, riconoscibili in relazione all'esecuzione della prestazione lavorativa, comprese quelle ricavabili dalla corrispondenza elettronica rientrano nell'ambito applicativo del principio di riservatezza trattato dalle suddette direttive della CE, anche se la corrispondenza, quindi lo scambio

[41] Sitzia, Andrea, Domenico Pizzonia. "*Il controllo del datore di lavoro su Internet e posta elettronica: quale tutela per la riservatezza sul luogo di lavoro?*." *LA NUOVA GIURISPRUDENZA CIVILE COMMENTATA* 6 (2016): 901-908.

di mail in questione sia avvenuto in piattaforme (hardware) di proprietà dell'azienda, messe a disposizione del lavoratore nell'esercizio della sua attività lavorativa.[42]

Come già detto, la disciplina sulla tutela della privacy non esclude del tutto la possibilità del datore di accedere alla casella di posta del lavoratore, né di verificare se egli la stia utilizzando per fini estranei alla prestazione dell'attività lavorativa e quindi per scopi personali, ma lo obbliga a fornire una informativa e una raccolta del consenso dell'interessato al trattamento dei dati, detta policy.

Ciò che è imprescindibile è il consenso del lavoratore sia all'informativa, sia alla policy aziendale che può prevedere la possibilità di monitoraggio della corrispondenza dei dipendenti. Dal lato del datore, l'acquisizione di suddetto consenso informato, permette di accedere alla casella di posta del lavoratore e di utilizzare, nei limiti stabiliti dallo Statuto dei lavoratori e dal Codice della privacy, le informazioni utili nella gestione del rapporto di lavoro ed eventualmente utili anche dal punto di vista disciplinare.[43]

3.3 SENTENZA N. 28378/2023 DELLA CORTE DI CASSAZIONE: "L'UTILIZZO DI INVESTIGATORI PRIVATI NEI CONTROLLI DIFENSIVI"

Con la presente Sentenza, la Corte di Cassazione si esprime in merito ad un tema di grande interesse ed allo stesso tempo molto controverso, quale l'utilizzo da parte del datore di lavoro dei dati raccolti dagli investigatori privati nell'ambito dei controlli difensivi svolti sull'attività lavorativa dei dipendenti.

Si definiscono "controlli difensivi" quei comportamenti messi in atto dal datore di lavoro con il fine di individuare dei comportamenti illeciti posti in essere dal lavoratore. Essi sono una fattispecie giurisprudenziale elaborata dalla vecchia formulazione dell'articolo

---

[42] Sitzia, Andrea, Domenico Pizzonia. "*Il controllo del datore di lavoro su Internet e posta elettronica: quale tutela per la riservatezza sul luogo di lavoro?*." *LA NUOVA GIURISPRUDENZA CIVILE COMMENTATA* 6 (2016): 901-908.

[43] Sitzia, Andrea, Domenico Pizzonia. cit.

4 dello Statuto dei Lavoratori, in vigore fino al 2015, prima della riforma messa in atto dal Jobs Act.

Nelle possibilità di controllo concesse al datore di lavoro rientrano proprio i controlli difensivi, che si identificano come quell'attività preposta ad accertare comportamenti illeciti ed allo stesso tempo lesivi del patrimonio aziendale e più in generale dell'immagine dell'azienda stessa. Essi rappresentano una vera e propria deroga all'articolo 4 dello statuto: a questo proposito lo stesso articolo 4 offre una serie di tutele volte a proteggere i lavoratori, impedendo al datore l'impiego di strumenti audiovisivi al fine di controllare l'attività lavorativa senza che vi sia una previa autorizzazione delle organizzazioni sindacali o dell'ispettorato del lavoro; un'altra importante garanzia attribuita dallo stesso articolo prevede, inoltre, che questa forma di controllo oltre ad essere autorizzata formalmente, debba sottostare ad una qualificata e fondata esigenza dell'azienda: identificabile in una esigenza di natura organizzativa, piuttosto che produttiva o di sicurezza dei lavoratori ed infine l'esigenza di tutelare il patrimonio aziendale. Quanto detto sta a significare che, prima di procedere effettuando i controlli difensivi, il datore di lavoro dovrà nutrire ragionevoli dubbi ed incertezze supportati da sospetti fondati, affinché gli sia concessa l'autorizzazione a procedere.

Il caso affrontato dalla Suprema Corte si sviluppa attorno alla controversa questione dell'utilizzo, da parte del datore di lavoro, dei dati raccolti da degli investigatori privati nell'ambito dei controlli difensivi.

L'oggetto della contestazione era il licenziamento intimato per ragioni disciplinari dal datore di lavoro (nello specifico Telecom Italia spa) al lavoratore che veniva licenziato per essersi assentato ed essersi dedicato numerose volte ad attività personali, mentre si sarebbe dovuto trovare a lavorare sul campo, in quanto era inquadrato nel V livello del contratto collettivo nazionale di telefonia, con mansioni di tecnico "on field", non operava quindi presso una sede di lavoro specifica, ma si recava presso il cliente o l'impianto per cui doveva svolgere le proprie mansioni.

Il lavoratore aveva pertanto impugnato il licenziamento di fronte al Tribunale di Milano, il quale aveva inizialmente accolto la tesi del licenziamento illegittimo, poiché ritorsivo, con una serie di motivazioni: in primis perchè questo licenziamento risultava illegittimo se comparato ad un caso simile, in cui il fatto era stato punito con una sanzione conservativa, evidenziando una sproporzione fra i due trattamenti; in secundis perchè

secondo quanto sostenuto dal lavoratore la società aveva fatto ricorso a dei controlli investigativi abusivi, disposti nei sui confronti, con conseguente inutilizzabilità dei fatti emersi, poichè ottenuti illegalmente. Sulla base di questo il Tribunale ordinava il reintegro nella società del sig. Garavaglia insieme ad un risarcimento pari alle retribuzioni maturate a partire dal licenziamento fino all'effettiva reintegrazione del lavoratore.

A questo punto Telecom Italia spa procede con il ricorso in appello e la situazione in un certo qual modo si ribalta: la Corte d'Appello, infatti, respinge tutte le domande dell'ormai ex dipendente e lo condanna a restituire quanto percepito in esecuzione della sentenza di primo grado. Gli viene contestata la falsa attestazione di tempi e modi di esecuzione dell'attività lavorativa ed emerge che egli avrebbe lavorato per un numero di ore inferiore al dovuto ed avrebbe svolto incombenze legate alla sua sfera personale durante l'orario di lavoro; viene smontata la tesi dell' intento punitivo nel suo licenziamento, comparata con il caso simile del collega, punito con una sanzione conservativa. Inoltre viene comprovata la motivazione della richiesta di controlli investigativi, sulla base di sospetti fondati nei confronti di Garavaglia, egli infatti secondo la società non avrebbe mai fornito delle motivazioni o delle spiegazioni che giustificassero le sue condotte, le sue mancanze nello svolgimento dell'attività lavorativa o per le incombenze di natura personale svolte all'interno dell'orario di lavoro.

Per tutti questi motivi, quindi viene meno il rapporto di fiducia tra datore di lavoro e lavoratore e per tanto viene confermato il licenziamento dell' ex dipendente.

Avverso tale sentenza, il ricorrente Garavaglia Walter ha quindi proposto ricorso in Cassazione, sollevando per la prima volta la questione che il sistema del software "WFM" (Work Force Managemnet) , usato per registrare gli orari di lavoro, fosse in realtà un illegittimo strumento di controllo a distanza, lamenta inoltre che sia mancata la prova della necessaria informativa al lavoratore, in violazione dell'articolo 4 comma 3 dello Statuto dei Lavoratori, ne consegue inevitabilmente anche il mancato rispetto del Decreto Legislativo 196/2003 (Codice in materia di protezione dei dati personali).

Il comma 3 dell'articolo 4 dello Statuto dei Lavoratori disciplina il ricorso, da parte del datore di lavoro, a strumenti di controllo indiretto dei lavoratori, stabilendo che le informazioni raccolte sono utilizzabili per tutti i fini connessi al rapporto di lavoro, a condizione però, che venga fornita ai dipendenti un'adeguata informativa. Secondo il

ricorrente, a mancare era proprio l'informativa e questo faceva in modo che i dati raccolti con l'uso del software WFM fossero inutilizzabili durante le indagini.

A tal proposito la Corte ritiene che i dati raccolti non siano frutto di un controllo a distanza (art 4), bensì di un'indagine e di conseguenza respinge la tesi di illegittimità dei dati raccolti, mossa dal ricorrente. La corte nega, quindi, che non sia pertinente il richiamo all'articolo 4 dello Statuto dei lavoratori.

La Corte aggiunge, inoltre che nel caso di specie vi fosse un "fondato sospetto" , il quale starebbe alla base e sarebbe una giustificazione alle indagini avviate dalla società nei confronti del dipendente; queste considerazioni escludono quindi anche l'applicabilità degli articoli 2 e 3 dello Statuto dei lavoratori (guardie giurate e personale di vigilanza), affermando che " le disposizioni dell'articolo 2 dello Statuto dei Lavoratori, nel limitare la sfera di intervento di persone preposte dal datore di lavoro a tutela del patrimonio aziendale, non precludono a quest'ultimo di ricorrere ad agenzie investigative, purché non sconfinino nella vigilanza dell'attività lavorativa vera e propria, riservata dall'articolo 3 dello Statuto".

Nel caso specifico, la condotta tenuta da Garavaglia è stata connotata da frode, ovvero era presente l'intenzione di ingannare e danneggiare la società arricchendosi alle sue spalle.

La posizione della Corte appare, invece, diversa rispetto alla mozione del ricorrente riguardante la violazione delle Regole Deontologiche commessa da Telecom Italia spa.

Garavaglia infatti, solleva la questione della violazione dell' articolo 8 comma 4 del Codice Deontologico, relativo al provvedimento del Garante della privacy n. 60 del 06/11/2008, allegato A. 6 al D.Lgs 196/2003 "Regole deontologiche relative ai trattamenti dei dati personali effettuati per svolgere investigazioni difensive o per far valere o difendere un diritto in sede giudiziaria".

L'articolo 8 dispone al comma 4 che "l'investigatore privato deve eseguire personalmente l'incarico ricevuto e può avvalersi solo di altri investigatori privati indicati nominativamente all'atto del conferimento dell'incarico, oppure successivamente in calce ad esso qualora tale possibilità sia stata prevista nell'atto di incarico".

Nel caso di specie di questa sentenza, la Cassazione stabilisce che il difetto nelle modalità di svolgere l'investigazione da parte di Telecom spa era stata per l'appunto una violazione delle Regole Deontologiche previste dal Garante della privacy: nella lettera di incarico

redatta dalla società (Telecom) che a sua volta incaricava una società di investigazione esterna, non erano stati riportati i nomi degli investigatori che avrebbero effettivamente effettuato l'indagine: ciò è stato ritenuto sufficiente, nonostante fosse un difetto di natura puramente formale, a compromettere la legittimazione dei soggetti incaricati che avevano acquisito i dati e le informazioni , decretandone l'inutilizzabilità assoluta ai fini probatori. Come citato nella sentenza, tale inutilizzabilità assoluta determina l'impossibilità sia per il datore di lavoro di porre i dati a fondamento di una contestazione disciplinare e poi di produrli in giudizio come mezzo di prova, sia per il giudice di porli a fondamento della sua decisione.

Infine la Corte dichiara "assorbito" il ricorso del sig. Garavaglia verso la violazione e la falsa applicazione degli articoli 2, 3, 4, 8, 18 dello Statuto dei Lavoratori, per avere la Corte Territoriale ritenuto legittime le indagini investigative , nonostante fossero attinenti all'adempimento della prestazione lavorativa.

In conclusione, con la presente sentenza la Corte si propone di rimarcare il valore normativo dei codici deontologici, i quali devono necessariamente essere un monito per il datore di lavoro che non deve trascurare il tema della privacy dei lavoratori anche nell'ambito dei controlli difensivi: si evince che è imprescindibile il rispetto dei limiti nel condurre le indagini, nel rispetto dei principi enunciati nello Statuto dei Lavoratori e nel Codice della privacy, che svolgono funzione di limite e di garanzia per i lavorato. Qualsiasi datore, infatti deve trattare i dati personali dei suoi dipendenti nel rispetto della dignità e della riservatezza, pena l'inutilità probatoria degli stessi.

CONCLUSIONI

In un periodo storico come quello in cui viviamo al giorno d'oggi è di fondamentale importanza che la disciplina del diritto del lavoro segua di pari passo l'evoluzione delle nuove tecnologie e degli strumenti tecnologici ed automatizzati, sempre più diffusi ed alla portata di tutti.

Se da un lato l'utilizzo degli strumenti di lavoro, quali pc, smartphone e tablet, facilitano notevolmente lo svolgimento dell'attività lavorativa, rendendola più "agile" e più "snella", dall'altro lato necessita di una regolazione efficace per far si che venga utilizzata nella maniera più corretta possibile. Un passo in avanti, in tal senso è stato fatto grazie alla riforma del Jobs Act. È altresì necessario stabilire dei limiti al controllo datoriale nel rispetto della privacy del lavoratore, anche qualora dovesse sussistere un sospetto legittimo e fondato di attività illecita, infatti tale controllo dovrà sempre attenersi al rispetto dei principi di proporzionalità e di necessità, nel rispetto della dignità del lavoratore ed assicurandogli un trattamenti giusto ed equo.

In conclusione possiamo dire che nell'ottica di un sistema in cui, sempre maggiormente sarà necessario il ricorso alle nuove tecnologie all'interno degli ambienti di lavoro, l'uso di tali strumenti dovrà essere direttamente proporzionale alla rispetto della privacy del lavoratore con la possibilità di effettuare controlli leciti da parte del datore a tutela della sua azienda e del suo patrimonio, nel rispetto della disciplina dello Statuto e del Codice della privacy a livello nazionale e nel rispetto del Regolamento 679/2016 a livello comunitario.

BIBLIOGRAFIA

- A. Del Ninno. *In vigore la riforma dell'art. 4 dello Statuto dei Lavoratori sui controlli a distanza: privacy dei lavoratori e nuove regole.* in www.dirittoegiustizia.it. 2015

- Bellavista Alessandro, Santucci Rosario. "*Tecnologie digitali, poteri datoriali e diritti dei lavoratori*.", in "*La sorveglianza digitale del datore di lavoro*" a cura di A. Trojsi. Giappichelli, 2022, pag 71 ss

- *Il ruolo dell'agenzia investigativa nel controllo delle obbligazioni lavorative.* dirittoegiustizia.it. 2018

- *Corte di Cassazione, sez. Lavoro, sentenza n. 19922/16*

- Ziccardi, Giovanni. *"Il controllo delle attività informatiche e telematiche del lavoratore: alcune considerazioni informatico giuridiche." Labour & Law Issues* 2.1 (2016): 57-58.

- Faleri, Claudia. *"Attività investigativa e accesso ai dati personali del lavoratore." Labour & Law Issues* 9.2 (2023): 25-27.

- Tortora, Adriano. "*Il nuovo regolamento europeo per la protezione dei dati (GDPR) e la figura del Data Protection Officer (DPO): incidenza sulla attività della pubblica amministrazione*." *Amministrativ@ mente-Rivista di ateneo dell'Università degli Studi di Roma "Foro Italico"* 5-6 (2018).

- F. Girolami *"Diritto alla privacy:protezione e regole per il trattamento dei dati personali del lavoratore nel settore privato*" Monotema n. 8/2017, pag 4

- R. Sciaudone "*Commentario al Codice della privacy*" Pacini Giuridica, 2023. in "*Raccolta di dati e pertinenza*" a cura di E. Pesaresi. pag 365 ss

- M. Soffientini "*Geolocalizzazione e impatto privacy*". Wolters Kluwer Italia s.r.l. 2017 pag 891

- S. Borghi "*Decisioni automatizzate e profilazione: le indicazioni dei Garanti Europei*" www privacy.it 2017

- Aimo, Mariapaola. *"Dalle schedature dei lavoratori alla profilazione tramite algoritmi: serve ancora l'art. 8 dello Statuto dei lavoratori?*". *Lavoro e diritto* 35.3-4 (2021): 593-596

- D. Bianchi *"Algoritmo reputazionale e consenso alla privacy. Basta una spiegazione nella lingua comune*". www.dirittoegiustizia.it 2023

- F. Paolucci "*Consenso, intelligenza artificiale e privacy"* www.medialaws.eu 2021
- R. Sciaudone "*Commentario al Codice della privacy*" Pacini Giuridica, 2023. in "*Garanzie in materia di controllo a distanza*" a cura di M. De Bernart. pag 398 ss

- P. Salazar "*Trattamento dati personali e rapporto di lavoro*: ecco com'è cambiata la disciplina" www.altalex.com 2018

- Borrillo, Barbara. "*La tutela della privacy e le nuove tecnologie: il principio di accountability e le sanzioni inflitte dalle Autorità di controllo dell'Unione europea dopo l'entrata in vigore del GDP*R." *Diritti fondamentali* 2 (2020): 344-345.

- Alvino, Ilario. "*I nuovi limiti al controllo a distanza dell'attività dei lavoratori nell'intersezione fra le regole dello Statuto dei lavoratori e quelle del Codice della privacy*." *Labour & Law Issues* 2.1 (2016) pag. 7ss

- I.Borrelli *"Controllo a distanza dei lavoratori*" www.wikilabour.it

- L. Giannini, *"Sistemi di rilevazione delle presenze in azienda: guida pratica alla compliance*" www.agendadigitale.eu , 2023

- "*Sospetto che dal pc aziendale del lavoratore sia partito un virus*: lecito per il datore effettuare un controllo", a cura di "La Redazione". www.dirittoegiustizia.it 2021

- Iaquinta, Francesca, and Alessandra Ingrao. *"La privacy e i dati sensibili del lavoratore legati all'utilizzo di social networks. Quando prevenire è meglio che curare*." *rel. ind* (2014). pag 19

- *"Lavoro: le linee guida del Garante per posta elettronica e internet*" 5 marzo 2007 [1387978] www.garantedellaprivacy.it

- R. Sciaudone "*Commentario al Codice della privacy*" Pacini Giuridica, 2023. in *"Garanzie in materia di controllo a distanza*" a cura di E. Pesaresi. pag 409

- Sitzia, Andrea, Domenico Pizzonia. "*Il controllo del datore di lavoro su Internet e posta elettronica: quale tutela per la riservatezza sul luogo di lavoro?*." *LA NUOVA GIURISPRUDENZA CIVILE COMMENTATA* 6 (2016): 901-908.