

Tutela penale della riservatezza e nuove tecnologie nel rapporto di lavoro: un binomio in continua evoluzione

di Riccardo Borsari e Francesco Falavigna

La tematica inerente alla tutela della sfera privata del lavoratore occupa tradizionalmente un ruolo di primissimo piano nella riflessione dottrinale e nella dimensione applicativa del diritto penale del lavoro; essa riflette, altresì, le difficoltà insite nell'adattamento all'odierno mondo digitale di normative costruite in un'epoca "analogica", e il conseguente scollamento fra diritto e realtà economico-sociale.

Volendo ripercorrere i tratti salienti dell'approfondimento svolto in un recente scritto pubblicato a inizio 2022 (R. Borsari, *La tutela penale del diritto alla riservatezza nel rapporto di lavoro*, in *Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro*, a cura di Carlo Pisani, Giampiero Proia e Adriana Topo, Giuffrè Francis Lefebvre), sin dagli anni Settanta del secolo scorso il compendio di norme della l. 20 maggio 1970, n. 300 (il c.d. "Statuto dei lavoratori") ha regolato – *forse con inconsapevole lungimiranza*, per rievocare le parole del prof. Francesco Santoni – i poteri organizzativi e di controllo del datore di lavoro, individuando le potenzialità lesive sottese all'utilizzo di strumenti, impianti e altre apparecchiature idonee al controllo a distanza negli ambienti di lavoro (art. 4), alla vigilanza (artt. 2-3), agli accertamenti sanitari (art. 5) e ai controlli sulla persona (art. 6), nonché alla raccolta d'informazioni, di dati personali e di notizie attinenti all'ambito extralavorativo (art. 8) e agli atti discriminatori (art. 15). Inoltre, il legislatore ha voluto presidiare tramite apposita sanzione penale (art. 38) le prescrizioni in questione, nella prospettiva della salvaguardia dei beni giuridici – oggetto di garanzia costituzionale – della libertà, dignità personale e sociale del lavoratore, cui la letteratura e l'elaborazione giurisprudenziale hanno affiancato, nell'assenza di una previsione esplicita all'interno della Costituzione, il diritto alla riservatezza quale vero e proprio diritto della personalità.

Il tema dei controlli, in special modo quelli a distanza, è negli ultimi anni tornato d'attualità a seguito delle modifiche che, dopo oltre quarant'anni di vita, hanno interessato le regole dettate dall'art. 4 dello Statuto per opera dell'art. 23 d.lgs. 14 settembre 2015, n. 151, nell'ambito dell'ampio intervento di riforma del mercato del lavoro nominato "*Jobs Act*".

Un rinnovamento della disciplina si era reso necessario in ragione dell'evoluzione tecnologica che ha caratterizzato la società e il mondo del lavoro specie dalla seconda metà degli anni Novanta, siccome testimoniato dall'ampio dibattito fra gli studiosi e dal susseguirsi delle pronunce giurisprudenziali che si sono via via profuse nello sforzo di conciliare la normativa del 1970 con l'avvento di mezzi (internet, posta elettronica, *tablet*, *smartphone*, *etc.*) assai diversi da quelli in presenza e in vista dei quali era stata concepita. Il divario tra il vecchio e il nuovo millennio si era infatti rivelato tale da ingenerare la percezione che l'art. 4 non fosse più in grado di realizzare un ragionevole temperamento fra l'interesse del datore di lavoro a controllare l'utilizzo da parte del lavoratore dei nuovi strumenti tecnologici aziendali e la tutela dei diritti fondamentali del lavoratore medesimo. E ciò, essenzialmente, in quanto il ricorso generalizzato alle nuove tecnologie, da un lato ha reso inattuale l'imposizione di vincoli potenzialmente interdittivi all'impiego di strumenti medio tempore divenuti indispensabili per rendere la prestazione lavorativa; dall'altro, ha ampliato la capacità di sorveglianza dell'attività,

accrescendo enormemente i poteri del datore di lavoro e, nel contempo, limitando significativamente l'effettiva portata dei diritti alla dignità, libertà e riservatezza dei lavoratori.

La riforma del “*Jobs Act*” ha dunque tentato di adeguare la disciplina dei controlli a distanza all'evoluzione tecnologica per trovare un (nuovo) punto di equilibrio tra le istanze implicate; senza peraltro trascurare l'esigenza di allineamento con l'imponente trasformazione della normativa generale in materia di *privacy* e riservatezza ormai risalente al d.lgs. 30 giugno 2003, n. 196 (cd. “Codice *Privacy*”).

Trascorsi alcuni anni dall'entrata in vigore del d.lgs. 151/2015, è peraltro diffusa l'impressione che pure la nuova disciplina stenti a stare al passo con la continua evoluzione tecnologica che permea la materia, alla quale si è di recente affiancata la riforma della normativa in tema di *privacy* e protezione dei dati ad opera del Regolamento (UE) n. 679/2016 e del relativo d.lgs. 10 agosto 2018, n. 101 di adeguamento.

Appartiene infatti all'ambito delle evidenze che il diritto del lavoro è intrinsecamente legato alle innovazioni tecnologiche, basandosi su un contratto connesso funzionalmente alle esigenze produttive e strutturato in modo da plasmare i contenuti del rapporto in funzione dei mutamenti organizzativi e produttivi.

Come anticipato, il lavoratore è oggi tenuto a utilizzare strumenti come il computer, lo *smartphone*, il *tablet* e, in generale, tutti i congegni analoghi forniti dalle aziende e dotati di connessione internet e/o localizzatore GPS. Sono divenuti di uso comune i dispositivi elettronici indossabili (cd. *wearables*), tra cui i più noti sono gli *smartwatch* e i *fitness band* (braccialetti “intelligenti”). Le auto aziendali sono solitamente dotate di GPS integrato, connessione a internet e *Telepass* per entrare e uscire dall'autostrada. Le comunicazioni aziendali viaggiano attraverso la posta elettronica e possono essere inviate e ricevute dal computer, dallo *smartphone* e dallo *smartwatch*.

Più di recente, anche la messaggistica istantanea si è insinuata nel mondo del lavoro: si pensi all'applicazione *WhatsApp* e alle varie opzioni di utilizzo, ivi comprese quelle che consentono la creazione di chat di gruppo e il controllo sull'avvenuta ricezione e lettura dei messaggi.

La rivoluzione tecnologica ha coinvolto anche la sede fisica in cui i lavoratori svolgono la prestazione lavorativa. In genere, essa dispone infatti, tra l'altro, di una rete internet locale (LAN), di *server* o di sistemi di conservazione dei dati collegati tra loro e di programmi che permettono l'accesso da remoto e l'interazione tra collaboratori.

Il datore di lavoro ha a disposizione programmi in grado di verificare con estrema precisione chi, come, quando e dove ha eseguito qualunque operazione che passa attraverso i *server* aziendali e, più in generale, di strumenti di controllo fondati sulla raccolta dei dati, dal più semplice al più complesso (si pensi alla biometria e agli strumenti che “robotizzano” il potere direttivo).

Anche i *social network* si sono evoluti in strumenti ad uso lavorativo, divenendo luoghi ove attingere a una serie di informazioni personali che difficilmente sarebbero state altrimenti accessibili ai datori di lavoro o ai reclutatori, dando così impulso alla nascita di nuove figure professionali (si pensi agli *influencer*, che sponsorizzano *brand* e prodotti sui *social* il cui guadagno dipende dai “like” ai *post* e dalle visualizzazioni di video e *stories*, oppure ai *social media manager*).

Quanto sinora assai sinteticamente delineato non esaurisce certo gli innumerevoli progressi tecnologici in atto: occorre infatti tenere conto pure della quarta rivoluzione industriale – digitale e robotica –, al fine di valutarne l'impatto sul lavoro e sulle sue regole. Le tecnologie innovative (*big data*, *cloud computing*, *cyber* sicurezza, internet delle cose, realtà aumentata, *blockchain*, intelligenza artificiale, *machine learning*, robotica e algoritmi) sono caratterizzate dall'intreccio tra digitalizzazione, automazione e, a monte, dallo strapotere dell'algoritmo che si serve di mezzi di esecuzione automatici estremamente veloci.

Un'ulteriore spinta verso la digitalizzazione del mondo del lavoro è stata impressa dalla recente crisi sanitaria legata alla pandemia da Covid-19. La sospensione improvvisa e inaspettata della gran parte delle attività ha accelerato il ricorso alla tecnologia per continuare a operare da remoto. Ne sono derivati un utilizzo crescente dello *smart working* e dei *web meeting* attraverso le varie piattaforme a disposizione

(Teams, Zoom, Meet, Webex e molti altri), nuove forme di controllo e una digitalizzazione estrema delle procedure che, con tutta probabilità, sarà, almeno in parte, mantenuta anche a emergenza cessata.

Lo sviluppo tecnologico, in un contesto di generale “sorveglianza”, ha oltremodo acuito le criticità connesse alla questione del controllo del datore di lavoro sull’attività svolta dal lavoratore, in origine essenzialmente circoscritto all’utilizzo di videocamere a circuito chiuso visionabili in differita.

È ad esempio possibile monitorare l’accesso fisico dei lavoratori in azienda grazie alla biometrica o alle tessere magnetiche, nonché l’accesso “virtuale” ai *server* e al *cloud* aziendali; conoscere il traffico internet dei dipendenti; apprendere dove è stato il lavoratore, quando ci è andato, che strada ha percorso e in quanto tempo, con chi ha parlato al telefono; acquisire dati sensibili (opinioni religiose e politiche, orientamento sessuale, stato di salute, *etc.*) pubblicati sui *social network* e utilizzarli a fini disciplinari e/o processuali, oppure nelle fasi di selezione, gestione e cessazione del personale. La tecnologia consente persino di “predire” i futuri comportamenti dei lavoratori mediante l’analisi “ragionata” dei numerosissimi dati a disposizione con l’aiuto dell’intelligenza artificiale e, di conseguenza, assumere decisioni basate su comportamenti che il lavoratore non ha ancora posto in essere.

L’evoluzione tratteggiata ha reso evidente l’inadeguatezza della disciplina statutaria, testimoniata anche dall’ampio confronto fra gli studiosi e dal susseguirsi di pronunce giurisprudenziali che si sono via via profuse nello sforzo di armonizzazione con l’avvento di mezzi assai diversi da quelli per i quali era stata concepita.

Tuttavia, benché il divario tra il vecchio e il nuovo millennio si fosse da lungo tempo manifestato in tutta la sua dirompente portata, nemmeno l’approvazione del “*Jobs Act*” ha compiutamente risolto le questioni sul tappeto, sicché il dibattito connesso a questa delicata materia appare ben lungi da un apprezzabile assestamento.

L’impianto originario delle fattispecie penali a presidio della riservatezza del lavoratore si è evoluto con le prime criticità applicative che hanno condotto all’elaborazione della controversa categoria dei “controlli difensivi” e alla crisi della disciplina dei controlli a distanza determinata dall’affievolirsi della distinzione tra strumenti di lavoro e strumenti di controllo, dal contrasto giurisprudenziale sull’ammissibilità dei controlli difensivi e dal necessario adeguamento del sistema dei controlli alla normativa *privacy*.

La riforma del “*Jobs Act*” ha così apportato significative novità e, in particolare, l’introduzione della finalità di tutela del patrimonio aziendale tra quelle per cui sono ammessi i controlli a distanza (previo accordo con le rappresentanze sindacali o autorizzazione amministrativa), la derogabilità della disciplina ordinaria per gli strumenti di lavoro e di registrazione degli accessi e delle presenze, la nuova regolamentazione dell’utilizzabilità delle informazioni raccolte e le modifiche all’apparato sanzionatorio nel campo dell’art. 171 del Codice *Privacy*.

Si mantengono a tutt’oggi articolate le posizioni della dottrina e della giurisprudenza anche sovranazionale sottese alle perduranti controversie in tema di controlli difensivi e sulla rilevanza del consenso del lavoratore al controllo a distanza.

Il fulcro del dibattito resta tuttavia incentrato sul rapporto in continua evoluzione tra tutela penale della riservatezza e nuove tecnologie nel rapporto di lavoro, del quale pure si occupa il recente scritto sopraccitato.

A seguito della riforma del “*Jobs Act*”, è anzitutto sorto l’interrogativo se nelle nozioni di «strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa» e di «strumenti di registrazione degli accessi e delle presenze», alle quali si riferisce la previsione derogatoria del secondo comma dell’art. 4 dello Statuto, possano essere annoverati – ed eventualmente in che termini – gli **strumenti biometrici**.

Il GDPR definisce i dati biometrici come «i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l’identificazione univoca, quali l’immagine facciale o i dati dattiloscopici» (art. 4, co. 1, n. 14). Sono tali, ad esempio, l’immagine dell’impronta digitale, l’immagine dell’iride o

della retina, la registrazione vocale, la tipografia della mano, la firma grafometrica, la dinamica di apposizione della firma, il tipo di andatura, *etc.*

Trattandosi di dati che pongono in stretta relazione il corpo e l'identità di un soggetto, essi tradizionalmente godono di una tutela rafforzata da parte dell'ordinamento. E, difatti, il GDPR li ha ricompresi tra le particolari categorie di dati dei quali è di regola vietato il trattamento, tranne che per particolari ipotesi come, per l'appunto, quando esso «è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato» (art. 9).

Prima della riforma del 2015, il Garante per la protezione dei dati personali si era a più riprese espresso sull'impiego di questi sistemi, anche con specifico riferimento al rapporto di lavoro. In particolare, dopo averne sancito l'illiceità dell'uso generalizzato e incontrollato, l'Autorità ha affermato che l'adozione di sistemi biometrici basati sull'elaborazione dell'impronta digitale o della topografia della mano può essere consentita per limitare l'accesso ad aree e locali ritenuti "sensibili" in cui è necessario assicurare elevati e specifici livelli di sicurezza, oppure per consentire l'utilizzo di apparati e macchinari pericolosi ai soli soggetti qualificati e specificamente addetti alle attività (Deliberazione 12 novembre 2014, n. 513, in www.garanteprivacy.it).

Dopo la riforma del "*Jobs Act*", l'Istituto Nazionale del Lavoro, con Circolare n. 5 del 19 febbraio 2018 («Indicazioni operative sull'installazione e utilizzazione di impianti audiovisivi e di altri strumenti di controllo ai sensi dell'art. 4 della legge n. 300/1970, in www.ispettorato.gov.it»), nel prendere le mosse da quanto precedentemente affermato dal Garante, ha precisato che «il riconoscimento biometrico, installato sulle macchine con lo scopo di impedire l'utilizzo della macchina a soggetti non autorizzati, necessario per avviare il funzionamento della stessa, può essere considerato uno strumento indispensabile a "... rendere la prestazione lavorativa ..." e pertanto si possa prescindere, ai sensi del comma 2 dell'art. 4 della l. 300/1970, sia dall'accordo con le rappresentanze sindacali sia dal procedimento amministrativo di carattere autorizzativo previsto dalla legge».

Ne deriva che, sulla base dei citati pronunciamenti, non incorre in responsabilità penale il datore di lavoro il quale, ricorrendone i presupposti, installa impianti che trattano dati biometrici senza esperire le procedure del primo comma dell'art. 4 dello Statuto.

In senso contrario all'utilizzo dei sistemi biometrici dev'essere peraltro segnalato il recente provvedimento del Garante *privacy* del 19 settembre 2019 («Parere su uno schema di decreto del Presidente del Consiglio dei ministri concernente la disciplina di attuazione della disposizione di cui all'articolo 2 della legge 19 giugno 2019, n. 56, recante "Interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo"», norma che prescriveva l'introduzione di sistemi di verifica biometrica dell'identità e di videosorveglianza degli accessi, in sostituzione dei diversi sistemi di rilevazione automatica in uso).

L'Autorità ha manifestato dubbi circa la compatibilità della legge sulla biometria nel settore pubblico rispetto alla disciplina europea e nazionale in materia di protezione dei dati personali poiché, a suo avviso, non conforme al canone della proporzionalità così come interpretato dalla giurisprudenza europea. Ed invero, la Corte di Giustizia ha più volte affermato che le esigenze di controllo non possono mai annullare e prevaricare il diritto alla riservatezza delle persone fisiche, dovendo sempre essere rispettato il principio di proporzionalità, cardine della tutela dei dati personali. Anche la Corte costituzionale ha enucleato principi analoghi proprio con riguardo al diritto alla protezione dei dati personali e rilevando che il test di proporzionalità si articola in una duplice valutazione: da un lato, sul carattere non sproporzionato degli oneri imposti rispetto ai legittimi fini perseguiti; dall'altro, sulla scelta della misura meno restrittiva dei diritti coinvolti.

In questa prospettiva, l'astratta, generalizzata e indifferenziata presunzione (fissata dall'art. 2 l. 56/2019) di sussistenza, per tutte le amministrazioni pubbliche, di fattori di rischio tali da far ritenere il sistema biometrico l'unico in grado di assicurare il rispetto dell'orario di lavoro non appare compatibile con il

principio di proporzionalità. A parere del Garante, il contrasto non viene sanato nemmeno riferendo il rispetto del canone di proporzionalità alle specifiche modalità attuative dell'obbligo di rilevazione biometrica (modulando diversamente, ad esempio, le tipologie di dati utilizzati o il termine di conservazione), soluzione che consentirebbe, al più, di ridurre l'impatto sul diritto alla protezione dei dati degli interessati, ma non di eliminare il vizio che connota in radice la norma, giacché «l'incompatibilità di tale previsione con i principi di proporzionalità, non eccedenza, minimizzazione risiede infatti nell'*an* prima che nel *quomodo* del trattamento: nella sua configurazione come astrattamente obbligatoria a prescindere da qualsiasi esigenza concreta e specifica in tal senso».

Le obiezioni del Garante hanno colto nel segno e portato alla mancata adozione del decreto citato, nonché all'abrogazione dei commi dell'art. 2 l. 56/2019 in materia di biometria ad opera della l. 30 dicembre 2020, n. 178 ("Legge di Bilancio 2021").

Alla luce di tali recenti evoluzioni, non può escludersi un mutamento di prospettiva a ispirazione sovranazionale verso una maggiore tutela del diritto alla riservatezza dei lavoratori nel trattamento dei dati biometrici. A tale riguardo, è appena il caso di evidenziare che i sistemi di accesso ai locali aziendali fondati sulla biometria, oltre ad acquisire una mole cospicua di dati con importanti ricadute in ottica *privacy*, possono nella sostanza consentire anche il controllo sull'attività svolta (ad esempio, sugli spostamenti del singolo dipendente all'interno dell'azienda) e, quindi, amplificare le ben note problematiche emerse in relazione all'utilizzo dei badge.

Altra questione problematica in continua evoluzione è quella inerente al rapporto tra i controlli del datore di lavoro e le modalità di svolgimento della **prestazione lavorativa a distanza**. Nel recente periodo, siffatta tipologia di lavoro ha goduto, com'è noto, di una crescita repentina ed esponenziale quale strumento volto a fronteggiare l'emergenza epidemiologica da **Covid-19**, con evidenti difficoltà di coordinamento rispetto alla normativa dell'art. 4 dello Statuto e del Codice *Privacy* sul piano del *contact tracing* e, più in generale, dei controlli nel rapporto di lavoro.

L'improvviso incedere della pandemia ha rappresentato una situazione indubbiamente eccezionale per l'estensione della misura e per la sovrapposizione tra fonti del diritto: difatti, la normativa emergenziale ha assunto a disciplina di riferimento la l. 81/2017 in materia di lavoro agile quale modalità ordinaria nel settore pubblico e privato per far fronte all'impossibilità di tutti i lavoratori di recarsi contemporaneamente nei luoghi di lavoro, da attuarsi con facoltà di deroga e pure in assenza di accordi individuali. Tale ultima eccezione ha lasciato nella pratica assai spesso indefinite le modalità di regolamentazione degli aspetti riguardanti le forme di esercizio del potere direttivo del datore di lavoro, gli strumenti utilizzati dal lavoratore, l'individuazione dei tempi di riposo nonché le misure tecniche e organizzative necessarie per assicurare la disconnessione dello *smart worker* dalle strumentazioni tecnologiche di lavoro. Nella specie, se si pensa al caso del lavoratore che installa sul proprio computer personale (modalità c.d. BYOD – "*Bring Your Own Device*") tutti gli strumenti necessari per svolgere l'attività lavorativa, si pone la questione di garantirne la riservatezza rispetto ai poteri di controllo del datore di lavoro, ivi compresa l'accessibilità alle informazioni estranee al rapporto o al rispetto dell'orario di lavoro.

In relazione alla specifica problematica del rapporto tra potere di controllo e protezione dei dati del personale dipendente si sono individuate in letteratura alcune questioni cruciali.

Una su tutte riguarda la perimetrazione del controllo nell'esecuzione della porzione "agile" della prestazione, giacché, ai sensi del secondo comma dell'art. 4, i controlli sugli strumenti di lavoro, seppure utilizzati in ambito domestico, non richiedono l'esperimento della procedura autorizzatoria di cui al primo comma. La tutela della riservatezza resta dunque essenzialmente affidata alla normativa in materia di trattamento dei dati personali fissata dal Regolamento 2016/679/UE e dal codice *privacy*, che peraltro, oltre ai ben noti doveri di informativa, all'art. 115 obbliga il datore di lavoro a garantire al lavoratore il rispetto della sua personalità e della sua libertà morale nell'ambito del rapporto di lavoro domestico, e il lavoratore a mantenere la necessaria riservatezza per tutto quanto si riferisce alla vita familiare. In argomento, merita peraltro evidenziare il protocollo d'intesa tra l'Ispettorato Nazionale del Lavoro e il Garante *privacy* sottoscritto il 22 aprile 2021 per l'avvio di una reciproca collaborazione istituzionale

nella gestione dei processi di digitalizzazione dei sistemi di gestione dell'organizzazione del lavoro, della produzione e dell'erogazione dei servizi, con particolare riferimento al sempre più frequente ricorso a modelli di prestazione "a distanza" dell'attività lavorativa (ad es., *dad*, *smart working*) e all'adozione di strumenti tecnologici per contenere il rischio di contagio, in ambito lavorativo pubblico e privato (ad esempio, applicazioni da installare su dispositivi mobili indossabili o su *smartphone*).

Su tale complessa e stratificata disciplina si innesta l'interrogativo sulla sorte dei controlli difensivi, che, laddove se ne ammetta la legittimità pure a seguito della riforma del "*Jobs Act*", possono riguardare anche i comportamenti illeciti posti in essere dal lavoratore agile; la normativa d'emergenza, del resto, ha disposto un divieto di procedere a licenziamenti collettivi, ma non ha introdotto limitazioni al potere disciplinare, fatte salve le espresse "scusanti" relative a particolari ragioni d'assenza dal lavoro dovute all'emergenza (si vedano, in particolare, gli artt. 23 e 47, comma 2, d.l. 18/2020, «Misure di potenziamento del Servizio sanitario nazionale e di sostegno economico per famiglie, lavoratori e imprese connesse all'emergenza epidemiologica da COVID-19»).

Merita un rapido accenno anche il tema del tracciamento digitale dei contatti (o *contact tracing*) finalizzato al contrasto della diffusione del Covid-19 effettuato all'interno del rapporto di lavoro. Al riguardo, il Garante *privacy* ha chiarito, nel Provvedimento di autorizzazione al trattamento dei dati personali effettuato attraverso il Sistema di allerta Covid-19 - App Immuni del 1° giugno 2020, che il Sistema nazionale di tracciamento digitale dei contatti finalizzato al contrasto della diffusione del virus è complementare alle modalità di tracciamento dei contatti ordinarie già in uso nell'ambito del Servizio sanitario nazionale (SSN) e consente, mediante la App Immuni installata liberamente e volontariamente dagli interessati, di avvisare tempestivamente gli utenti di essere stati a contatto con un soggetto risultato positivo al Covid-19, fornendo indicazioni e raccomandazioni sul comportamento da tenere.

Anche il tracciamento digitale dei contatti sul luogo di lavoro può pertanto integrare una forma di controllo a distanza dei lavoratori – attuata attraverso *wearables device* o dispositivi installati dai datori di lavoro sugli impianti – rientrando tra gli altri strumenti che, secondo il primo comma dell'art. 4 dello Statuto, possono essere impiegati, previa mediazione sindacale e/o amministrativa, per finalità di sicurezza del lavoro. Si pensi, in particolare, all'ipotesi in cui gli applicativi utilizzati (App Immuni o altri) consentano di tracciare gli spostamenti all'interno dell'azienda mediante identificazione del singolo lavoratore e di quelli con cui lo stesso sia venuto in contatto.

Sempre in tema di Covid-19, è appena il caso di evidenziare che alcune disposizioni previste nei protocolli emanati sulla base della normativa emergenziale consentono al datore di lavoro di trattare dati sulla salute dei lavoratori in deroga al divieto fissato dall'art. 5 dello Statuto e sanzionato penalmente dall'art. 38 dello Statuto medesimo. Ad esempio, oltre alla facoltà di rilevazione in tempo reale della temperatura corporea, sono state introdotte procedure per la gestione di casi sintomatici che presuppongono la conoscenza da parte del datore di lavoro dello stato morboso del dipendente, il quale può procedere direttamente alla comunicazione (avendo l'obbligo di segnalare al datore di lavoro qualsiasi situazione di pericolo per la salute e la sicurezza sui luoghi di lavoro), oppure i sintomi manifestatisi all'ingresso della sede di lavoro o durante la prestazione lavorativa. In tali ipotesi, è legittimo il trattamento da parte del datore di lavoro dei dati relativi ai sintomi o alla positività al Covid-19 del lavoratore per la finalità di salute e sicurezza dei luoghi di lavoro o per adempiere agli obblighi di collaborazione con gli operatori di sanità pubblica senza incorrere in sanzioni penali e amministrative.

Al medesimo riguardo, va pure considerato l'obbligo di possedere e mostrare su richiesta il *Green pass* nei luoghi di lavoro, pubblici e privati, introdotto dal d.l. 21 settembre 2021, n. 127 a decorrere dal 15 ottobre 2021. Nella specie, i controlli sono demandati al datore di lavoro, il quale è tenuto ad adottare misure operative affinché nei locali aziendali accedano solo i lavoratori muniti di certificazione verde, ivi compresa la designazione formale dei soggetti incaricati dell'accertamento delle violazioni degli obblighi. L'inottemperanza agli obblighi organizzativi e di controllo da parte del datore di lavoro e l'accesso al luogo di lavoro in assenza di *Green pass* da parte del lavoratore comportano l'applicazione di sanzioni amministrative pecuniarie, oltre alle ulteriori sanzioni disciplinari previste dalla Contrattazione Collettiva di settore. Ai sensi del d.l. 7 gennaio 2022, n. 1, inoltre, dal 15 febbraio 2022

l'accesso ai luoghi di lavoro da parte dei lavoratori con età pari o superiore a 50 anni è subordinato alla previa verifica in ordine al possesso del *Green pass* "rafforzato".

Questioni delicate sono poi sollevate dai wearables device, dispositivi che rappresentano una delle frontiere tecnologiche più importanti di "Industria 4.0" e che nel rapporto di lavoro possono essere utilizzati agli scopi più disparati: in particolare, per prevenire eventi lesivi per la salute e la sicurezza (ad esempio, sulla presenza di sostanze tossiche in misura superiore a quella consentita), oppure per finalità di training (si pensi ai *Google glasses*, che potenziano le capacità di apprendimento aumentando virtualmente la realtà). Essi possono tuttavia costituire anche uno strumento per misurare l'efficienza del lavoratore sul posto di lavoro, magari per il tramite di indicatori dei parametri vitali (l'attività cardiaca, le calorie assunte e quelle bruciate, le ore di sonno e quelle di veglia, *etc.*) attraverso cui conoscerne a distanza lo stato d'animo e valutarne la *performance*. D'altro canto, a differenza di dispositivi come computer, *smartphone* e *tablet*, i *wearables device* sono concepiti per essere sempre in funzione, anche qualora l'utente svolga altre attività.

Pure con riguardo a tali dispositivi si pone pertanto l'esigenza di individuare e delimitare gli scopi legittimi idonei a giustificare il controllo a distanza, quale può essere la necessità di ridurre le frodi o finalità premiali o formative. Inoltre, occorre che il controllo sia attuato compatibilmente ai principi generali e comunque con modalità idonee a prevenire il rischio di lesione della dignità e dei diritti fondamentali attraverso controlli continui, anelastici e indiscriminati come quelli di cui si tratta, peraltro spesso motivati da esigenze preventive e non attuali.

L'orientamento del mondo giuridico è di estrema prudenza, anche a fronte delle enormi implicazioni sottese all'ingresso, nel mondo del lavoro e nella disponibilità dei datori di lavoro, delle informazioni che i *wearables* sono in grado di raccogliere e trasmettere. Sul punto, in particolare, si è espresso il Garante *privacy* il 28 febbraio 2019 a chiusura di un procedimento avviato nei confronti di una società di raccolta rifiuti che aveva dotato i dipendenti preposti al servizio di spazzamento su strada di dispositivi indossabili sul polso (tipo "braccialetto") muniti di GPS, con i quali effettuare la lettura delle etichette elettroniche collocate sui cestini getta rifiuti e segnalare l'eventuale spostamento di quelli non ancorati al suolo. L'Autorità, pur nel reputare tale configurazione non in contrasto con i principi di necessità e proporzionalità del GDPR rispetto alle finalità perseguite dalla società, e ponendo l'accento sul principio di responsabilizzazione, ha tuttavia ritenuto necessario individuare ulteriori misure maggiormente rispettose della dignità dei lavoratori, su tutte la stipula di un accordo sindacale ai sensi del primo comma dell'art. 4 dello Statuto (costituente condizione di liceità del trattamento).

Anche la definizione del regime giuridico dei *wearables* nel rapporto di lavoro non può allora che passare attraverso l'interpretazione della nozione di «strumento di lavoro» a fondamento della deroga alla necessità delle procedure autorizzatorie del secondo comma dell'art. 4, su cui, come si è detto, si registrano posizioni variegata in dottrina e in giurisprudenza, alle quali si aggiungono quelle di vari attori istituzionali. Evidentemente, nelle ipotesi in cui essi possano essere intesi come strumenti necessari per lo svolgimento dell'attività lavorativa, il datore di lavoro si gioverà dell'operatività del comma secondo della disposizione, anche ai fini difensivi.

La riservatezza del lavoratore è messa a dura prova pure dall'utilizzo dei *social network*, sia come forma di controllo a distanza, nella misura in cui il datore di lavoro può verificarne l'indebito utilizzo durante l'espletamento delle mansioni, sia soprattutto come strumento per la raccolta di informazioni funzionali alla selezione del personale e all'accesso al lavoro o financo all'esercizio del potere disciplinare. Trattasi di forme di utilizzo assai frequenti, che tendono ad esulare dal perimetro di applicazione dell'articolo 4 dello Statuto, con impatto sulla tutela della riservatezza e sull'apparato di norme allestito a tal fine.

La rapida diffusione della blockchain chiama poi l'interprete a stabilire se la stessa si configuri, ai fini dell'art. 4 dello Statuto, come strumento di controllo o di lavoro, laddove impiegata nell'ambito del rapporto su piattaforma digitale. Tale tecnologia, in un primo momento utilizzata come base della struttura operativa di *Bitcoin* e criptovalute, sta profondamente influenzando i servizi digitali e trasformando i modelli aziendali in molteplici settori; essa attualmente rappresenta, tra l'altro, un

importante strumento di monitoraggio delle vicende giuridiche di beni, servizi e diritti, in quanto offre elevati livelli di tracciabilità e sicurezza nelle transazioni online.

Si ritiene in letteratura che la qualificazione della *blockchain* in termini di strumento di controllo o di lavoro dipenda dalla funzione per la quale il datore di lavoro su piattaforma vi fa ricorso, esattamente come avviene per qualunque altro programma digitale. Nella specie, richiamando l'interpretazione del Garante *privacy* e del Ministero del Lavoro secondo cui nella nozione di strumento di lavoro vanno ricompresi solo i servizi, *software* o applicativi, strettamente funzionali alla prestazione lavorativa, anche sotto il profilo della sicurezza (come il servizio di posta elettronica e gli altri servizi della rete aziendale, compreso il collegamento a Internet, idonei a garantire un elevato livello di sicurezza della medesima per il lavoratore), la tecnologia *blockchain* può essere annoverata tra gli strumenti di lavoro diretti ad assicurare un elevato livello di sicurezza della rete aziendale, purché effettivamente impiegata per l'esecuzione della prestazione; viceversa, essa si configura quale strumento di controllo e, quindi, deve essere assoggettata ai requisiti del primo comma dell'art. 4 dello Statuto.

Ulteriori riflessioni meritano l'utilizzo dei dati dei lavoratori a fini di **profilazione e decisione automatizzata**, unitamente alle informazioni provenienti dal contesto lavorativo, e le "forme" sempre nuove di intelligenza artificiale alimentate dalla forte accelerazione delle attività di *big data analytics* e *data mining*.

La profilazione è un fenomeno trattato dalla dottrina giuridica soltanto in tempi recenti e che ha trovato una definizione compiuta nel 2016 attraverso il GDPR. Invero, l'incedere della tecnologia ha fatto gradualmente emergere la percezione in ordine alla crescente capacità di elaborazione dei dati degli utenti da parte dei vari fornitori di servizi, inducendo anche il legislatore italiano ad allestire delle prime modalità di tutela rafforzata.

Intesa come raccolta di dati personali che trascende il singolo individuo, la profilazione può essere applicata al contesto lavorativo e utilizzata per "prevedere" le decisioni e i comportamenti dei lavoratori (*recte*: stimarne le probabilità di realizzazione), nonché, soprattutto, per automatizzare (parzialmente o totalmente) le decisioni relative alla gestione delle risorse umane.

Se, così, si è già messo in luce come le forme di controllo perpetrabili dal datore di lavoro trovino copertura solo parziale nella disciplina dello Statuto, i limiti della tradizionale tutela giuslavoristica sono ancora più evidenti in rapporto alle tecnologie di automatizzazione. Il meccanismo è difatti in grado di "retroagire" rispetto ai dati raccolti creando ulteriori informazioni, metterle in relazione con quelle già a disposizione e creare un "profilo" analogo a quello del soggetto controllato. Per questa via, grazie agli ultimi sviluppi dati dal *machine learning*, è possibile riprodurre le decisioni umane in svariati ambiti applicativi, con risultati talvolta molto superiori in termini di precisione, velocità, completezza, adattabilità. Se tali operazioni potrebbero a prima vista non apparire problematiche, il fenomeno assume tuttavia peculiare rilevanza quando la categorizzazione dell'individuo in un gruppo piuttosto che in un altro comporta una decisione che influisce sul godimento dei diritti.

Focalizzando l'attenzione sul possibile utilizzo dello strumento della profilazione nel contesto dei controlli datoriali sui lavoratori, si osserva allora che il datore di lavoro, grazie ai dati raccolti, può sviluppare programmi in grado di prevedere decisioni future del dipendente (ad esempio, se egli sta valutando di lasciare la sua posizione), di indirizzarlo nella sua crescita professionale (per esempio, rispetto a un avanzamento di carriera oppure a un cambio di sede), sino ad avvalersi in tempo reale dei dati delle conversazioni elettroniche intrattenute coi colleghi al fine di valutarne l'affiatamento e la motivazione (attraverso, ad esempio, l'analisi della frequenza dei messaggi e del tipo di vocabolario utilizzato).

Questo meccanismo di decisione automatizzata, denominato *automated decision making*, è a tutt'oggi privo di definizione normativa.

Di qui è possibile comprendere il rischio insito in tali forme di trattamento e, in generale, in tutte le procedure automatizzate, vale a dire quello di neutralizzare la libertà di scelta dell'individuo e mettere in crisi il sistema di tutele della riservatezza del lavoratore, poiché il datore di lavoro può accumulare più

informazioni persino al di là della propria consapevolezza. Estremizzando tale scenario, il lavoratore rischia che il datore di lavoro possa adottare decisioni pregiudizievoli nei suoi confronti non soltanto in relazione a una valutazione negativa sulla *performance* individuale *in fieri*, ma pure sulla base della concordanza tra circostanze o situazioni estrinseche all'attività lavorativa, anche solo indirettamente correlate tra loro, del quale egli stesso ignora l'esistenza, o addirittura prendendo a riferimento situazioni ancora non verificatesi (ma che, secondo l'algoritmo, si verificheranno).

Evidente che, come per i *social network*, l'ambito del controllo può travalicare i confini lavorativi intaccando la sfera intima della persona.

La tematica del ruolo delle decisioni automatizzate nel rapporto di lavoro è strettamente connessa a quella degli strumenti avanzati utilizzati per la gestione delle risorse umane e, in particolare, lo *smart recruitment*.

Ci si riferisce, anzitutto, agli agenti artificiali che scansionano i curricula dei candidati o i loro profili *on line* sulla base di requisiti predeterminati o *pattern* psicologico-sociali, allo scopo di perfezionare la scelta del personale e, al contempo, sveltire le procedure di assunzione, rivolgendo l'attenzione solo a candidati i quali, con alte probabilità, saranno idonei e/o interessati alla mansione loro offerta.

Ancora, sono stati elaborati e attuati strumenti con cui l'algoritmo possa interagire direttamente con i candidati (tramite *chat-bot*), analizzandone in tempo reale le risposte, il tono di voce, le espressioni del viso al fine di ricavare informazioni sulla personalità o indirizzarli verso la posizione più adatta, con l'obiettivo dichiarato di consentire una più efficace attività di selezione, che si svolge senza limiti di tempo e di luogo, in qualunque momento della giornata e, soprattutto, azzerando il rischio che la valutazione dei candidati sia condizionata da pregiudizi di carattere psicologico, ideologico o culturale intrinseci nel selezionatore umano. Tali tecniche possono essere applicate anche da remoto e consentono di raccogliere una quantità sempre maggiore di dati.

Siffatte procedure automatizzate possono agevolmente influire sulla determinazione dei contenuti del contratto di lavoro o sulla strategia da adottare nella gestione del relativo rapporto in ragione di fattori che il lavoratore non può né controllare né anticipare. Ad esempio, esse sono in grado di determinare il compenso minimo che il candidato sarebbe disposto ad accettare, consentendo all'azienda di evitare proposte più alte del minimo che il lavoratore è disposto ad accettare e, quindi, riducendo sensibilmente i costi per il personale. Ancora, mediante questa procedura automatizzata di selezione si può stabilire preventivamente il grado di affidabilità del candidato o di collaborazione con gli altri dipendenti, funzione che si presta ad essere utilizzata per evitare di assumere lavoratori potenzialmente problematici (incompetenti, disonesti, instabili), che, secondo l'algoritmo, probabilmente, in futuro, potrebbero creare difficoltà all'azienda.

In buona sostanza, l'applicazione concreta di tecnologie di intelligenza artificiale sul terreno dei rapporti di lavoro si pone in aperta tensione con la disciplina statutaria e la *ratio* di tutela dei diritti fondamentali che la ispira: pare dunque imprescindibile un intervento legislativo auspicabilmente organico volto a ricomporre il delicato sistema di compenetrazione tra contrapposti interessi.

Seguendo la medesima prospettiva, alcuni spunti *de jure condendo* derivano dal raffronto con la normativa processualpenalistica, ove apprezzabili sforzi di avvicinamento alle più recenti spinte evolutive si registrano nelle nuove discipline dei più moderni strumenti d'indagine (sul punto, si rimanda alla lettura dello scritto summenzionato).