IL TRATTAMENTO DEI DATI PARTICOLARI NELL'AMBITO DEL RAPPORTO DI LAVORO: DATI GIUDIZIARI E SANITARI

Breve sintesi del piano d'indagine

Il presente lavoro intende analizzare nel **primo capitolo** il trattamento dei dati particolari nel rapporto di lavoro prendendo le mosse da un necessario approfondimento storico e definitorio del diritto alla riservatezza sin dalle sue origini, con particolare attenzione al dibattito nel nostro Paese, in dottrina e giurisprudenza, che ha contribuito a fornire rango costituzionale al diritto alla riservatezza. Prosegue con un esame puntuale delle nozioni e dei principi relativi ai dati personali e particolari insieme ad uno specifico approfondimento sul concetto di trattamento, che sui dati particolari assume un carattere peculiare.

Successivamente si passa all'esame del diritto alla riservatezza nella disciplina speciale del rapporto di lavoro che trova nello Statuto dei lavoratori un impianto normativo pionieristico a tutela del lavoratore, in particolare sul divieto di indagini sulle opinioni e sui controlli a distanza.

Si proseguirà con l'analisi del trattamento dei dati dei lavoratori nella disciplina legislativa europea e nazionale formatasi nell' ultimo decennio a cui sono seguiti gli interventi in materia sia del Garante nazionale che dei Garanti europei, oggetto di specifica indagine.

Il **secondo capitolo** si incentra sul trattamento dei dati giudiziari del lavoratore nel rapporto di lavoro e in particolare sul fatto che, pur essendo questi ultimi normati sia dal GDPR che dal Codice della privacy, manca tutt'ora nel nostro Paese una legge, un regolamento o un decreto del Ministro della Giustizia necessario ad autorizzare e disciplinare il trattamento di tali dati. Lo studio intende analizzare le possibili soluzioni proposte sia in dottrina che dagli esperti del settore per colmare tale vuoto normativo. Parallelamente verrà analizzato il trattamento dei dati giudiziari nel settore bancario e assicurativo, che, grazie a una recente disciplina speciale, può vantare una sua regolamentazione.

Successivamente lo studio si sofferma sul trattamento di questa particolare categoria di dati del lavoratore sia all'atto della sua assunzione che nel corso del rapporto di lavoro con l'analisi di giurisprudenza di merito e di legittimità particolarmente significativa.

Infine, nel **terzo capitolo** si ricostruisce la nozione e il trattamento dei dati sanitari del lavoratore nella normativa europea e nazionale, analizzando anche alcuni casi concreti in tema di protezione della riservatezza dei dati sanitari del lavoratore. Lo studio intende poi soffermarsi con particolare attenzione sulla emergenza sanitaria dovuta alla pandemia da COVID-19 e alle numerose ed evidenti implicazioni in tema di riservatezza derivanti dall'aggravarsi della situazione di emergenza sanitaria.

Il lavoro si conclude da una parte con l'analisi del Protocollo d'intesa tra il Governo italiano e le parti sociali e sulle importanti implicazioni dello stesso sul trattamento dei dati sanitari, e dall'altra con le recenti pronunce dei Garanti privacy europei e del Garante italiano sulla disciplina emergenziale in tema di trattamento dei dati sanitari.

CAPITOLO I

Il trattamento dei dati dei lavoratori

SOMMARIO: 1. Definizioni e principi in materia di diritto alla riservatezza. - 1.1. Il diritto alla riservatezza: evoluzione e rilevanza costituzionale. - 1.2. Il dato personale. - 1.3. Il dato particolare. - 1.4. Il trattamento dei dati: nozione. - 1.4.1. I principi applicabili al trattamento dei dati. - 1.4.2. Il trattamento di categorie particolari di dati. - 2. La tutela del diritto alla riservatezza nel rapporto di lavoro. - 2.1. La tutela del diritto alla riservatezza nello Statuto dei lavoratori. 2.1.1. Il divieto di indagini sulle opinioni. - 2.1.2. I controlli a distanza. 2.2. Il trattamento dei dati dei lavoratori nel Regolamento generale per la protezione dei dati personali n. 2016/679 (GDPR). - 2.3. Il trattamento dei dati dei lavoratori nel Codice della privacy come modificato dal D.Lgs. n. 101 del 2018. 2.4. Il trattamento dei dati personali dei lavoratori nell'interpretazione del Garante della privacy italiano. 2.5. Il trattamento dei dati personali dei lavoratori nell'interpretazione dei Garanti europei: l'*opinon* n. 2 del 2017 del Gruppo di lavoro articolo 29.

1. Definizioni e principi in materia di diritto alla riservatezza

Il concetto che esista una sfera intangibile della persona riguardante la sua vita privata è molto antico e già Aristotele distingueva tra *polis*= sfera politica - pubblica, e *oikos* = sfera privata, associata alla famiglia e alla vita domestica. La stessa idea è efficacemente riassunta nelle parole che già nel 1766, Lord Chatham, Primo ministro inglese, pronunciò di fronte al Parlamento in merito ai confini tra i poteri pubblici (quelli della Corona) e la sfera privata dell'individuo: "Il più povero degli uomini può nella sua casetta lanciare una sfida opponendosi a tutte le forze della corona. La casetta può essere fragile, il suo tetto può essere traballante, il vento può soffiare da tutte le parti, la tempesta può entrare e la pioggia può entrare, ma il re d'Inghilterra non può entrare; tutte le sue forze non osano attraversare la soglia di tale casetta in rovina" ([1]).

Le origini moderne del diritto alla riservatezza si possono far risalire a due giuristi statunitensi, Samuel Warren, e Louis Brandeis, nel saggio *The right to privacy,* pubblicato nel 1890 nella rivista americana *Harvard Law Review,* in cui affermano l'esistenza nell'ordinamento degli Stati Uniti del diritto in questione. Secondo gli autori "ognuno ha diritto di essere lasciato in pace, di proteggere quella che è la sfera più intima, così come ha diritto di proteggere e difendere, d'altrui invasioni, la sua proprietà privata" ([2]).

Meno conosciuto forse è il fatto che cinque anni prima Rudolf Von Jhering, illustre giurista tedesco, aveva sostenuto che i diritti privati soggettivi possono tutelare interessi non economici. L'occasione gli veniva offerta da una nuova tecnologia di quel tempo: la fotografia. Jhering, pur non parlando di diritto della personalità, affermava il diritto di una persona ad opporsi al

([1]) C. FARALLI, *Il diritto alla privacy. Profili storico-filosofici*, in *Persona e mercato dei dati. Riflessioni sul GDPR* (a cura di) N. GALGANO, Padova, CEDAM, 2019.
([2]) S. WARREN, L. BRANDEIS, *The right to privacy*, in *4 Harvard Law Review*, 1890 – 1891.

fatto che il proprio ritratto fosse esposto in vetrina dal fotografo o da lui venduto senza autorizzazione ([3]).

Nella nostra cultura giuridica la riservatezza, intesa come possibilità di godere pienamente della propria intimità, secondo Stefano Rodotà "è un connotato differenziale della borghesia rispetto ad altre classi". In sostanza, il borghese si appropria di un suo spazio con un meccanismo volto a tutelare un diritto alla proprietà che potremmo definire "solitaria". Conseguentemente la nascita della riservatezza non è quindi la realizzazione di un'esigenza naturale di ogni individuo, ma si presenta come la acquisizione di un privilegio da parte di un gruppo.

Ben presto poi si spezzerà il nesso di identificazione con la classe borghese e la riservatezza diventerà un modo per reagire contro l'autoritarismo e contro una politica di discriminazione basata sulle opinioni politiche, sindacali, religiose, o di razza, evolvendosi verso la promozione della parità di trattamento tra i cittadini per realizzare l'eguaglianza tra di essi e non per custodire il privilegio di pochi ([4]).

È evidente, pertanto, come il diritto alla riservatezza nasca legato strettamente al diritto di proprietà, per collocarsi successivamente tra gli strumenti di tutela della personalità. Sempre più frequentemente questa tendenza a tutelare la sfera della vita privata della persona si configura poi come un diritto assoluto di libera determinazione nello svolgimento della personalità.

([3]) R. JHERING, *Recthsschutz gegen injuriose Rechtsverletzungen*, in *Jahrbucher fur die Dogmatik des heutigen romischen und deutschen Privatrechts*, XXIII, 1885, citato in P. SIRENA, *Il sequestro della stampa a tutela del diritto all'immagine*, in *Studi in onore di Giovanni Giacobbe, Vol. II* (a cura di) G. DALLA TORRE, Milano, Giuffrè, 2010.
([4]) S. RODOTÀ, *Riservatezza*, in *Enciclopedia Italiana*, VI Appendice, Istituto della enciclopedia italiana, Treccani, 2000.

1.1 Il diritto alla riservatezza: evoluzione e rilevanza costituzionale.

La Costituzione italiana del 1947, a differenza di Costituzioni europee più recenti, non contiene una disciplina esplicita o una disposizione specifica sul diritto alla riservatezza, ma prima in dottrina e poi in giurisprudenza si è ampliamente discusso sul fatto che molteplici norme costituzionali possano essere prese come indice del riconoscimento del rango costituzionale del diritto alla riservatezza.

I primi articoli da prendere a riferimento per fornire tutela costituzionale alla riservatezza sono gli articoli 2 e 3, rispettivamente sulla garanzia dei diritti inviolabili dell'uomo, sulla pari dignità sociale e sul pieno sviluppo della persona umana. La dottrina, interrogandosi sul possibile valore costituzionale del diritto alla riservatezza, ha dibattuto ampiamente la questione, che di seguito è così sinteticamente riepilogabile.

Sull' art. 2 la questione principale riguarda la possibilità che tale norma possa essere ritenuta una clausola generale aperta, tale da non considerare l'elenco dei diritti inviolabili di libertà costituzionalmente rilevati come un numero chiuso, basandosi sulla consapevolezza che la riservatezza assolve al fine superiore di apprestare effettiva tutela alla persona umana e alle sue esigenze fondamentali. Tra questi vi è chi, come Cataudella, ritiene che la riservatezza rientri nell'articolo 2 in quanto il riserbo costituisce una necessità addirittura biologica dell'uomo essendo questo un aspetto inalienabile della persona umana ([5]).

Altri analogamente affermano che la riservatezza svolge un ruolo basilare sul piano strumentale, e cioè, che sia la garanzia di una sfera sottratta alle intrusioni di terzi sia la sicurezza che determinate informazioni

([5]) A. CATAUDELLA, *Scritti giuridici*, Padova, CEDAM, 1991.

resteranno private, sono la condizione "per assicurare alla persona il pieno godimento dei diritti fondamentali sanciti dalla Costituzione" ([6]).

Diversamente, vi sono opinioni che dubitano sulla costituzionalizzazione del diritto alla riservatezza per il tramite dell'art. 2, e la condizionano all'accertamento positivo sull'inviolabilità dello stesso concludendo che la riservatezza non sembra possedere tale attributo. ([7]).

Inoltre, c'è chi critica l'articolo 2 come norma aperta, invocando una sentenza della Corte costituzionale, la n. 98 del 1979, "dove in tre righe è stato detto che l'elenco dei diritti di libertà contenuto nella Costituzione non può essere ampliato in via di interpretazione" ([8]).

Il diritto alla riservatezza è concettualmente collegato anche alla tutela della libertà personale e al principio di eguaglianza sostanziale sancito dall' art. 3 della Costituzione, e in tal senso la disposizione in questione è stata analizzata sia in riferimento al primo comma, in cui si parla di "pari dignità sociale" sia in riferimento al secondo, in cui è contenuto il concetto di garanzia del "pieno sviluppo della persona umana". Chi, come Valenti, supporta la tesi favorevole all'utilizzo dell'art. 3 come suggello costituzionale del diritto alla riservatezza ha accentuato la necessità della garanzia di una sfera privata inviolabile affinché la dignità e lo sviluppo della persona, siano effettivamente assicurati e non rimangano una semplice affermazione di principio ([9]).

([6]) A. BELVEDERE, *Riservatezza e strumenti di informazione*, in *Dizionario del diritto privato*, Milano, Vallardi, 1980.
([7]) S. FOIS, *Questioni sul fondamento costituzionale del diritto alla "identità personale"*, in AAVV, *L'informazione e i diritti della persona*, Napoli, Jovene, 1983.
([8]) A. PIZZORUSSO, *I profili costituzionali di un nuovo diritto della persona*, in AAVV, *Il diritto alla identità personale*, (a cura di) G. ALPA, M. BESSONE, Padova, CEDAM, 1981.
([9]) A.M. VALENTI, *La dignità umana quale diritto inviolabile dell'uomo: luci ed ombre nelle moderne esperienze internazionali e bioetiche nell'approssimarsi del terzo millennio*, Perugia, Università di Perugia, 1995.

Le posizioni che si sono invece dimostrate critiche circa la possibile tutela costituzionale della vita privata alla stregua dell'art. 3 si fondano sulle seguenti argomentazioni: taluni lamentano l'eccessiva genericità della disposizione costituzionale che non si presterebbe pertanto a tutelare un diritto così puntuale come quello della riservatezza ([10]). Altri si chiedono se sia veramente di ostacolo allo sviluppo della persona la conoscenza di notizie private e l'attacco alla sfera privata da parte soprattutto dei grandi mezzi di comunicazione di massa ([11]); infine, altri sostengono che il riferimento alla dignità sociale contenuto nel primo comma dell'art. 3 miri a tutelare in via diretta interessi diversi dalla riservatezza, identificabili più propriamente nel decoro e nella reputazione della persona ([12]).

Vi sono poi altre disposizioni costituzionali che vanno esaminate ai fini della attribuibilità o meno del rango costituzionale del diritto alla riservatezza, considerato che sanciscono l'inviolabilità della libertà personale (art. 13), del domicilio (art. 14), della libertà e segretezza della corrispondenza e di ogni altra forma di comunicazione (art. 15).

La posizione dominante in dottrina nega questa possibilità e afferma che tali disposizioni si riferiscono principalmente a diritti distinti da quello alla riservatezza, oppure ad aspetti settoriali e manifestazioni parziali di essa, o semmai a diritti qualificati "affini", come per esempio il diritto al segreto. Si registra pertanto un generalizzato sfavore verso l'utilizzo di questi principi come esclusivo sostegno del diritto alla riservatezza ([13]).

Ciò non esclude però che possano essere utilizzati in complementarità con gli articoli 2 e 3 della Costituzione; in effetti sia la giurisprudenza della

([10]) S. FOIS, *op. cit*.
([11]) F. BRICOLA, *Prospettive e limiti della tutela penale della riservatezza*, in AAVV, *Il diritto alla riservatezza e la sua tutela penale*, Milano, Giuffrè, 1970.
([12]) A. CATAUDELLA, *La tutela civile della vita privata*, Milano, Giuffrè, 1972.
([13]) F. BRICOLA, *op. cit*.; BELVEDERE, A., *op. cit*.

Corte costituzionale sia quella della Corte di Cassazione hanno operato in tal senso. Di seguito vedremo come.

Tutti i dubbi espressi in dottrina in merito al rango costituzionale del diritto alla riservatezza sono finalmente risolti dalla fondamentale pronuncia della Corte Costituzionale che, con sentenza 12/4/1973 n. 38 ([14]), decidendo sulla questione della legittimità delle misure cautelari *ex* art. 700 c.p.c dirette alle immagini fotografiche non ancora pubblicate ma destinate alla pubblicazione, qualora sia in gioco la tutela dei diritti inviolabili della persona, colloca il diritto alla riservatezza tra quelli inviolabili dell'uomo garantiti dalla Costituzione, richiamandosi anche all'art. 12 della "Dichiarazione Universale dei diritti dell'uomo" e all'art. 8 della "Convenzione europea dei diritti dell'uomo". Afferma la Corte: "Non contrastano con le norme costituzionali ed anzi mirano a realizzare i fini dell'articolo 2 affermati anche negli articoli 3, comma 2, e 13 comma 1, che riconoscono e garantiscono i diritti inviolabili dell'uomo, tra i quali rientra quello del proprio decoro, del proprio onore, della propria rispettabilità, riservatezza, intimità e reputazione, sanciti espressamente negli articoli 8 e 10 della Convenzione Europea sui diritti dell'uomo, gli artt. 10 del Codice civile…".

La Corte di Cassazione, con la sentenza del 27/5/1975 n. 2129 ([15]), il c.d. "caso Soraya", muta il suo precedente orientamento e si uniforma alla Corte costituzionale, sancendo definitivamente l'esistenza di un autonomo diritto alla riservatezza.

Il caso fu provocato dalla pubblicazione nel 1968 sul periodico "Gente" di un servizio fotografico, realizzato con teleobiettivo, da cui risultavano ripresi in vari atteggiamenti, anche molto intimi, il regista Franco Indovina e la principessa Soraya Esfandiari all'interno della villa di quest'ultima. La

([14]) Corte Cost., sent. 12/4/1973 n. 38, in *Gazzetta Ufficiale* n. 102, 18/4/1973.
([15]) Cass., sent. 27/5/1975, n. 2129, in *Foro italiano*, I, 1976.

Esfandiari lamentava la violazione del suo domicilio, della sua riservatezza e della sua immagine, con pregiudizio del decoro, dell'onore e della reputazione. Il fatto aveva anche un diretto risvolto economico, dal momento che alla principessa era stata attribuito un appannaggio a condizione che mantenesse una vita integra ed illibata.

La sentenza, che rappresenta il *leading case* in materia, costituisce il primo formale riconoscimento dell'esistenza del diritto alla riservatezza nel nostro ordinamento non più sulla base di una tutela derivante dall'art. 14 della Costituzione, che sancisce l'inviolabilità del domicilio, ma di un richiamo espresso agli articoli 2, 3, 27, 29, 41 Cost. quali norme da cui ricavare principi di "tutela della sfera privata del soggetto con conseguenti limitazioni ad altre garanzie costituzionali quali, per esempio, il diritto all'informazione".

Da quanto sopra detto emerge con evidenza che il diritto alla riservatezza abbia trovato accoglimento in Italia principalmente grazie al lavoro di dottrina e giurisprudenza, che hanno contribuito decisivamente non solo alla sua nascita, ma anche alla sua evoluzione, nel silenzio legislativo che, come noto, perdurerà fino alla prima legge sulla *privacy* del 1996.

1.2 Il dato personale.

Il 25 maggio 2018 in tutti gli Stati membri dell'Unione Europea entra in vigore il Regolamento UE n. 2016/679 noto come GDPR (General Data Protection Regulation) relativo alla protezione delle persone fisiche con riguardo al trattamento e alla libera circolazione dei dati personali. Come indicato dalla stessa Commissione europea, il GDPR nasce da specifiche esigenze di certezza giuridica, armonizzazione e maggiore semplicità delle norme riguardati il trasferimento di dati personali nell' UE e dalla UE verso altre parti del mondo. In tale Regolamento, recepito in Italia dal d.lgs. n. 101 del 2018, all'art. 4 troviamo la definizione di dato personale: "Qualsiasi informazione riguardante una persona fisica identificata o identificabile (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".

Occorre però fare un passo indietro per capire sinteticamente come si è arrivati a questa nozione di dato personale contenuta nel Regolamento comunitario.

Il primo Paese in Europa ad emanare una legge sui dati personali fu la Germania che nel 1977, con una legge federale sulla protezione dei dati, sentì il bisogno di normare la circolazione e proteggere gli stessi a seguito del significativo sviluppo delle banche dati e dell'informatizzazione dell'informazione ([16]).

([16]) G.A. BENOCCHIO, F. CASUCCI, (a cura di), *Temi e Istituti di Diritto Privato dell'Unione Europea*, Torino, Giappichelli, 2017.

Successivamente l'OCSE (Organizzazione per la cooperazione e lo sviluppo economico) nel 1980 emana le "Linee guida sulla protezione della vita privata e sui flussi transfrontalieri di dati di carattere personale", seguite l'anno successivo dal Consiglio d' Europa che approva la "Convezione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale".

Le motivazioni che spinsero il Consiglio d'Europa a emanare tale convenzione furono dettate da una triplice esigenza, e in particolare: - una unione più stretta tra i suoi membri nel rispetto della prevalenza del diritto nonché dei diritti umani e delle libertà individuali; - la necessità di estendere la protezione dei diritti e delle libertà fondamentali di ciascuno e in particolare il diritto al rispetto della vita privata, tenuto conto dell' intensificazione dei flussi internazionali di dati a carattere personale oggetto di elaborazione automatica; - la necessità di conciliare i valori fondamentali del rispetto della vita privata e della libera circolazione delle informazioni tra i popoli ([17]).

È quindi all'art. 2 che il Consiglio d'Europa per la prima volta definisce il dato a carattere personale, come: "ogni informazione concernente una persona fisica identificata o identificabile (persona interessata)".

Nel 1995 la Direttiva 95/46/CE del Parlamento Europeo e del Consiglio prosegue il percorso tracciato dal Consiglio d' Europa e integra la definizione di dato personale specificando i criteri e le modalità di identificabilità della persona all' art. 2: "Qualsiasi informazione concernente una persona fisica identificata o identificabile (persona interessata); si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero d'identificazione o ad uno o

([17]) Consiglio d' Europa, Convezione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, Strasburgo, 28/1/1981.

più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica , economica, culturale o sociale" ([18]).

In Italia la prima definizione in merito ai dati personali si ha con la legge 675/1996 "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali", che recepisce la predetta direttiva 95/46/CE con una dicitura che non ricalca puntualmente la definizione comunitaria, ma così la riassume: "Qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale".

La legge in questione veniva poi modificata qualche anno più tardi, nel 2003, con l'avvento del D.lgs. n. 196 (Codice in materia di protezione dei dati personali) e successivamente dalla legge 22/12/2011 n. 214, che ha eliminato le persone giuridiche, gli enti e le associazioni dalla definizione di dato personale, circoscrivendolo quindi alle sole persone fisiche.

Tale definizione di dato personale è quindi rimasta nel nostro ordinamento fino all'approvazione del Regolamento UE n. 2016/679, che come riportato a inizio paragrafo contiene, ad oggi, la definizione di dato personale vigente nel nostro ordinamento.

Va detto, peraltro, che la dicitura del Regolamento UE offre una definizione più dettagliata del termine, andando a specificare criteri di identificazione ulteriori rispetto al "numero di identificazione" della persona. Più in particolare i dati personali riguardano le informazioni riguardanti sia la vita privata di una persona (che comprende attività professionali e non) sia la vita pubblica.

([18]) Direttiva 95/46/CE del Parlamento europeo e del Consiglio, 24/10/1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, in *Gazzetta ufficiale delle Comunità europee* del 23/11/1995.

Le informazioni, infatti, contengono i dati riguardanti una persona, se un individuo è identificato o identificabile sulla base di tali informazioni, e se qualora non identificabile, sia comunque individuato attraverso tali informazioni in modo da consentire di svelare la sua identità conducendo ulteriori ricerche ([19]).

Va infine sottolineato che non è rilevante la forma in cui i dati personali vengono utilizzati o archiviati: sono dati, infatti, le comunicazioni scritte o orali, le immagini, le informazioni registrate attraverso i mezzi elettronici, i suoni, le informazioni su supporto cartaceo ([20]).

([19]) Agenzia dell'Unione Europea per i diritti fondamentali, Consiglio d'Europa, Garante europeo della protezione dei dati, (a cura di), *Manuale sul diritto europeo in materia di protezione dei dati*, 2018.
([20]) N. BERNARDI, (a cura di) *Privacy. Protezione e trattamento dei dati*, Milano, IPSOA, 2019.

1.3 Il dato particolare.

Il Regolamento UE n. 2016/679, tra le tante novità che ha apportato rispetto alla normativa previgente, introduce nel nostro ordinamento il concetto di "dato particolare", e più precisamente all'art. 9 par. 1, nel vietarne il trattamento, lo definisce in questo modo: "[...] dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale e all'orientamento sessuale della persona".

La fattispecie così identificata era già parzialmente nota sia al legislatore europeo che al legislatore italiano, che rispettivamente con la Direttiva 95/46/CE e con il Codice della privacy, emendato poi dal d.lgs. 101/2018, si riferivano ai c.d. "dati sensibili". In particolare, il legislatore italiano alla formulazione dell'art.4 lett.b del Codice della privacy li identificava come: "I dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale".

Ad una lettura più attenta possiamo notare come il Regolamento sia più specifico, dilatando i confini dei dati sensibili, e aggiungendo i dati genetici, i dati biometrici intesi ad identificare in modo univoco una persona, oltre a quelli relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona ([21]). Ciò non implica il fatto che l'utilizzo del temine dato sensibile sia scorretto, ma deve essere chiaro che la definizione cambia, poiché dalla

([21]) F. DI CIOMMO, *La privacy sanitaria*, in R. PARDOLESI, (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, Giuffrè, 2003.

entrata in vigore del GDPR ci si riferirà direttamente alla formulazione dell'art. 9 par.1 contenuta al suo interno.

Si ritiene utile in questa sede fare una specificazione sui dati genetici e sui dati biometrici, data la loro peculiarità. I dati genetici sono infatti quei dati che forniscono informazioni uniche sulla fisiologia o sulla salute di una persona fisica, e che risultano in particolare dalla analisi di un campione biologico della persona fisica in questione. I dati biometrici attengono invece alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentano l'identificazione univoca quali l'immagine facciale o i dati dattiloscopici.

Certamente il periodo di tempo trascorso tra la normativa italiana e quella comunitaria ha consentito al legislatore di maturare una certa esperienza dei casi, degli abusi e delle discriminazioni che si sono verificate nei diversi ambiti, senonché nel medesimo tempo la tecnologia ha dimostrato che la sua evoluzione può creare molteplici rischi per la tutela di informazioni personali e, tanto più, per determinate categorie di dati ([22]). In effetti sia i dati genetici che quelli biometrici vanno sottoposti a garanzie particolarmente puntuali, altrimenti, se divulgati, rischiano di determinare ripercussioni rilevanti sull'interessato, considerato che in essi "è racchiusa la dimensione individuale della persona, il modo di essere, di pensare e di interagire nelle relazioni sociali" ([23]).

Infine, sul tema della tassatività delle categorie particolari di dati così come elencate nell' art. 9, l'elenco è senz'altro da reputarsi come un numero

([22]) M. GRANIERI, *Il trattamento di categorie particolari di dati personali nel Reg. UE 2016/679*, in *Nuove leggi civili commentate*, Padova, CEDAM, 1/2017.
([23]) G. FINOCCHIARO, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Bologna, Zanichelli, 2012.

chiuso benché dalle singole voci sia possibile fornire una interpretazione estensiva ([24]).

([24]) R. TUCCILLO, *Art. 9 Regolamento UE n. 2016/679 – Trattamento di categorie particolari di dati personali*, in A. BARBA, S. PAGLIANTINI, (a cura di), *Commentario del Codice civile – Delle persone – Leggi collegate Vol. II*, Milano, UTET Giuridica, 2019.

1.4 Il trattamento dei dati: nozione.

La nozione di trattamento prevista all'art. 4, primo comma, punto 2) del GDPR non distinguendo tra dato personale e dato particolare, è la seguente: "Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione".

Per comprendere la definizione di trattamento è bene soffermarsi su quelle situazioni per cui il dato non è nella portata e nella disponibilità dell'interessato. Si usa ormai comunemente affermare che l'interessato non ha presso di sé il dato, in quanto il dato è presso altri, che lo trattano per lui. Si può trattare di condotte statiche del dato (come la semplice archiviazione) oppure di condotte dinamiche (come, ad esempio, l'elaborazione o la profilazione). La sintesi è che il trattamento è comunque un comportamento che merita una regolamentazione, deve essere significativo, e in quanto tale non può essere un accidente occasionale ma deve fondarsi su un atto volitivo ([25]).

([25]) N. BERNARDI, *op. cit*.

1.4.1. I principi applicabili al trattamento dei dati.

L' art. 5 del GDPR introduce i principi applicabili al trattamento dei dati personali, che sono così riepilogabili: liceità, correttezza, trasparenza, limitazione della finalità, minimizzazione, esattezza, limitazione della conservazione, integrità e riservatezza, responsabilizzazione.

Per ciascuno di essi vale la pena spendere qualche parola vista la rilevanza del tema.

Il principio di **liceità** implica che una limitazione alla protezione dei dati personali richiede una espressa previsione normativa ammissibile unicamente se la limitazione risulta funzionale al perseguimento di uno scopo legittimo e proporzionale.

La **correttezza** è da ricondurre a quella regola di buona fede che impone a chi tratta i dati dell'interessato di porre in essere tutti gli atti giuridici e/o materiali che si rendano necessari alla salvaguardia dell'interessato in modo da non comportare un apprezzabile sacrificio a suo carico ([26]).

Il principio di **trasparenza** richiede che l'interessato sia consapevole delle caratteristiche essenziali del trattamento anche al fine di agevolare l'esercizio dei propri diritti, primo fra tutti quello della regola del consenso ([27]).

Secondo quanto rilevato dai Garanti europei nelle linee guida sul principio di trasparenza redatte (Gruppo di lavoro Articolo 29), sono tre gli elementi centrali del principio di trasparenza: 1) la fornitura agli interessati di informazioni relative al corretto trattamento; 2) le modalità con le quali il

([26]) F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo, Vol. I*, Torino, Giappichelli, 2016.
([27]) F. RESTA, *Art. 5 in GDPR e normativa privacy*, (a cura di) G.M, RICCIO, G. SCORZA, E. BELLISARIO, Milano, IPSOA, 2018.

titolare del trattamento comunica con gli interessati riguardo ai diritti di cui godono ai sensi del regolamento; 3) Le modalità con le quali il titolare del trattamento agevola agli interessati l'esercizio dei diritti di cui godono ([28]).

La **limitazione della finalità** comporta che i dati personali debbano essere trattati e raccolti per scopi determinati e legittimi, richiedendo anche che detta finalità sia propriamente esplicita, si determina *ex ante* e costituisce una garanzia specifica per l'interessato da declinare in funzione della tutela dei suoi diritti ([29]).

Il principio di **minimizzazione** impone che i dati debbano essere adeguati, pertinenti e limitati. In particolare, la pertinenza richiede che il dato trattato sia in un rapporto di strumentalità rispetto allo scopo per cui è trattato. La limitazione impone di contenere i dati trattati a quelli indispensabili per il raggiungimento dello scopo perseguito.

L'**esattezza** richiede che i dati siano esatti e aggiornati, e impone che siano adottate misure ragionevoli per cancellare o rettificare i dati inesatti rispetto agli obiettivi per cui sono trattati.

Il principio di **limitazione della conservazione** richiede che il periodo di conservazione sia limitato al minimo necessario, tanto che, chi li tratta, dovrebbe stabilire un termine per la cancellazione o per la verifica periodica consentendo una conservazione prolungata nel tempo qualora i dati siano trattati per fini di archiviazione nel pubblico interesse, di ricerca scientifica, storica o a fini statistici.

I principi di **integrità e riservatezza** richiedono che i dati personali siano trattati garantendo un'adeguata sicurezza e adottando ogni precauzione

([28]) Gruppo di lavoro Art. 29, Linee Guida n. 260/2017 sul principio di trasparenza ai sensi del Regolamento n. 2016/679.
([29]) L. BOLOGNINI, E. PELINO, C. BISTOLFI, *Il Regolamento Privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali,* Milano, Giuffrè, 2016.

opportuna, volta anche ad impedire un accesso e un utilizzo non autorizzato dei dati nonché delle attrezzature impiegate per il trattamento. Tale previsione comporta uno specifico dovere di chi tratta i dati di rispettare il criterio di adeguatezza al fine di scongiurare trattamenti illeciti o non autorizzati, nonché la perdita, la distruzione e il danno dei dati personali trattati ([30]).

La **responsabilizzazione** (c.d. *accountability*), una delle principali novità introdotte dal GDPR,[31] secondo quanto risulta dal Considerando n. 74 del Regolamento, richiede che chi tratta i dati sia tenuto a mettere in atto misure adeguate, ed essere in grado di dimostrare la conformità delle attività di trattamento con il GDPR, anche per quanto concerne l'efficacia delle misure adottate.

([30]) D. ACHILLE, *Art. 5 Regolamento UE n. 2016/679 – Principi applicabili al trattamento di dati personali*, in BARBA, A., PAGLIANTINI, S., (a cura di), *Commentario del codice civile – Delle persone – Leggi collegate Vol. II*, Milano, UTET Giuridica, 2019.
([31]) G. FINOCCHIARO, *Introduzione al Regolamento europeo sulla protezione dei dati*, in *Nuove leggi civili commentate*, Padova, CEDAM, 1/2017.

1.4.2. Il trattamento di categorie particolari di dati.

Il GDPR, in tema di trattamento di categorie particolari di dati personali (art. 9 par. 2), detta una disciplina più specifica, in quanto materia delicata e sensibile, considerato, come già sopra accennato, che non riguarda soltanto la mera identificazione della persona, ma la sfera più intima dell'interessato e per questo motivo necessita di una tutela rafforzata e puntuale. Per fare ciò l'articolo in questione pone un generale divieto di trattamento, e in sostanza un principio di indisponibilità del diritto.

Tuttavia, per consentire il trattamento di questi dati elenca una molteplicità di deroghe ed eccezioni al generale divieto di trattamento previsto dal primo paragrafo.

Una prima ipotesi di liceità del trattamento dei dati particolari riguarda il consenso dell'interessato, che oltre ad avere una o più finalità specifiche, deve essere esplicito. A tale eccezione può accostarsi anche quella di cui alla lettera *e)* dell'art.9, ossia il trattamento dei dati personali che sono stati resi manifestamente pubblici dall'interessato. In ambedue le ipotesi, infatti, sia l'autodeterminazione del privato sull'utilizzo, sia la libertà di scelta sono i presupposti della liceità del trattamento.

Naturalmente, per quanto riguarda il consenso, l'interessato deve essere messo nelle condizioni di accettare o meno i termini proposti ovvero rifiutarli senza subire pregiudizio. In ambito lavorativo, invece, occorre ricordare che il consenso risulta essere manifestamente inadeguato in quanto, di norma, non liberamente espresso da parte del dipendente in considerazione della naturale debolezza dello stesso dinanzi al datore di lavoro. In sintesi, nel rapporto di lavoro il consenso non può essere ritenuto un "salvacondotto" per il trattamento dei dati personali e la tutela penale (fornita dall'art. 38 dello Statuto dei lavoratori) all'osservanza degli articoli 4 ed 8 dello stesso Statuto

conferma che il divieto assoluto ivi previsto non ammette deroghe, tantomeno con il consenso o con l'accordo tra le parti. Sempre in tema di consenso, occorre ricordare che il considerando 43 del GDPR specifica che per assicurare la libertà alla prestazione dello stesso, occorre che non vi sia un evidente squilibrio tra l'interessato e il titolare del trattamento, in particolare quando si tratta di un rapporto intrapreso con un'autorità pubblica.

Tra le ipotesi ulteriori di deroga al trattamento di categorie particolari di dati, vi rientrano i casi in cui il trattamento è necessario per finalità diverse relative al diritto del lavoro, alla sicurezza e protezione sociale, laddove, in presenza di determinate condizioni, il trattamento è reputato lecito.

Sul trattamento in materia di diritto del lavoro, naturalmente, si rimanda al paragrafo successivo, dove l'argomento verrà analizzato in maniera più specifica, in quanto oggetto principale di questa tesi.

Le attività svolte da fondazioni, associazioni o altri organismi che perseguono finalità politiche, filosofiche, religiose o sindacali senza scopo di lucro sono considerate ulteriori fattispecie di liceità del trattamento, così come i motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli stati membri.

La lettera *c)* dell'art. 9 introduce una deroga alla necessità di manifestazione del consenso al trattamento dei dati, consentendo il trattamento di quei dati necessari alla tutela della vita e dell'incolumità dell'interessato o di un terzo qualora vi siano casi di incapacità fisica o giuridica.

Altra deroga al trattamento è quella che consente la raccolta di dati ad opera di terzi soggetti che svolgano la funzione di investigatori privati, committenti dell'investigazione o necessitati a raccogliere materiale probatorio per l'esercizio di un diritto o per la difesa in giudizio.

Viene altresì ammesso il trattamento per finalità di assistenza sanitaria, medicina preventiva e del lavoro, nonché giustificato per ragioni di interesse pubblico relativo ad esigenze sanitarie per gravi minacce alla salute a carattere transfrontaliero o per garantire elevati parametri di qualità e sicurezza dell'assistenza sanitaria. Per quanto riguarda il trattamento dei dati sanitari si rimanda al successivo capitolo 3 per una disamina più specifica e approfondita.

Infine, vi è un'ultima categoria di trattamenti leciti che riguarda le finalità di archiviazione nel pubblico interesse di ricerca scientifica, storica o statistica. Tale deroga trova fondamento nella concezione della ricerca scientifica come una missione virtuosa capace di produrre effetti vantaggiosi per il pubblico in generale ([32]).

([32]) R. TUCCILLO, *Art. 9 Regolamento UE n. 2016/679 – Trattamento di categorie particolari di dati personali, op. cit*.

2. La tutela del diritto alla riservatezza nel rapporto di lavoro.

Fin qui è stato analizzato il diritto alla riservatezza, come, in sintesi, il diritto a conservare il possesso di sé e della propria identità. È indubbio, però, che tutta la dottrina civilistica ha inserito il diritto alla riservatezza tra i diritti della personalità, accomunandoli al fatto che ambedue fanno riferimento ad interessi non economici e proteggono la sfera personale dell'individuo ([33]).

Nel diritto del lavoro, invece, la tutela della riservatezza acquista una dimensione ulteriore, quella sociale, causata dal fatto che il lavoratore è un soggetto inserito in un rapporto giuridico col datore di lavoro,[34] aggravato dallo squilibrio di potere tra le parti, e dalla naturale debolezza del dipendente dinanzi al datore di lavoro ([35]). Nel contratto di lavoro, infatti, assume rilevanza la dignità sociale, oltre che la dignità umana, comprensiva non soltanto del riserbo individuale, ma anche della concreta sfera politica e sociale del singolo.

Non è un caso che il fondamento costituzionale del diritto alla riservatezza del lavoratore si può ricondurre nel nostro ordinamento, prima ancora che nello Statuto dei lavoratori, negli articoli 2, 3, 32 e, specialmente, 41, comma 2 della Costituzione. Tale norma, come noto, impone all'imprenditore/datore di lavoro di esercitare la sua posizione dominante dal punto di vista economico e contrattuale, senza ledere la "sicurezza", la "libertà" e la "dignità" umana del lavoratore.

([33]) P. RESCIGNO, *Il diritto all'identità della vita privata, in studi in onore di F. Santoro Passarelli, IV*, Napoli, Jovene, 1972.
([34]) L. MENGONI, *Introduzione al titolo I, in Commentario dello Statuto dei lavoratori* diretto da PROSPERETTI, U., Milano, Giuffrè, 1975.
([35]) R. DEL PUNTA, *Diritti della persona e contratto di lavoro* in *Giornale di diritto del lavoro e di relazioni industriali*, Milano, FrancoAngeli, 2006.

Viene pertanto tutelato e riconosciuto il diritto del lavoratore a non subire, anche in azienda, interferenze lesive della propria dignità ([36]).

([36]) F. SANTONI, *La privacy nel rapporto di lavoro: dal diritto alla riservatezza alla tutela dei dati personali*, in P. TULLINI, *Tecnologie della comunicazione e riservatezza nel rapporto di lavoro*, Padova, CEDAM, 2010.

2.1 La tutela del diritto alla riservatezza nello Statuto dei lavoratori.

Sul fondamento costituzionale del diritto alla riservatezza del lavoratore, sopra riepilogato, si è inserita la legislazione speciale contenuta nello Statuto dei lavoratori (legge 20/5/1970 n. 300), che vanta una autentica primazia nel riconoscimento di tale diritto in ambito lavoristico.

Lo Statuto, infatti, nella Relazione dell'allora Ministro del Lavoro Giacomo Brodolini che accompagnò la presentazione al Senato del disegno di legge n. 738/1969, contiene "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro".

Nella Relazione si afferma che: "Il proposito del disegno di legge che il governo si onora di presentare è di contribuire in primo luogo a creare un clima di rispetto della dignità e della libertà umana nei luoghi di lavoro, riconducendo l'esercizio dei poteri direttivo e disciplinare dell'imprenditore nel loro giusto alveo e cioè in una stretta finalizzazione allo svolgimento delle attività produttive" ([37]).

Sul presupposto della rilevanza di situazioni potenzialmente lesive della sicurezza, della libertà e della dignità umana dei lavoratori si era già espressa sia la Commissione parlamentare d'inchiesta sulle condizioni dei lavoratori in Italia nel 1959, sia nel marzo 1969 la X Commissione parlamentare de Senato, che aveva documentato forme di controllo occulto e poliziesco ai danni dei lavoratori ([38]).

([37]) Senato della Repubblica, V legislatura, Doc. n. 738, 2, 1969.
([38]) E. BARRACO, A. SITZIA*, Potere di controllo e privacy. Ed. I*, Milano, IPSOA, 2016.

Lo Statuto dei lavoratori si prese quindi la responsabilità e il carico di individuare principi in grado di risolvere situazioni antigiuridiche richiamate dal Parlamento. Nonostante l'ordinamento giuridico non avesse ancora adottato la categoria concettuale e il termine "riservatezza", lo Statuto dei lavoratori individua chiaramente, forse con inconsapevole lungimiranza, le potenzialità lesive insite nella raccolta di informazioni, riguardanti le opinioni politiche, religiose o sindacali del lavoratore e di notizie attinenti all'ambito extra lavorativo (art. 8) nonché l'utilizzo di strumenti, impianti, e altre apparecchiature idonee al controllo a distanza negli ambienti di lavoro (art. 4). Lo Statuto intende quindi fornire un'ampia tutela al lavoratore rispetto alle violazioni del datore di lavoro in questi ambiti e la rilevanza di questa tutela viene ulteriormente supportata dal fatto che, la violazione degli articoli menzionati, venga sanzionata penalmente dall' art. 38 dello Statuto non solo per l'azione in sé, ma anche per il semplice tentativo effettuato. Di contro, va sottolineato il fatto che l'onere di dimostrare l'avvenuta violazione è del lavoratore e tale onere non sempre è agevole per quest'ultimo.

2.1.1. Il divieto di indagini sulle opinioni

L'art. 8 dello Statuto, rubricato come "Divieto di indagini sulle opinioni", così afferma: "è 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 in esame, come già accennato, è una norma pionieristica, essendo il primo esplicito riconoscimento legislativo dell'esistenza di un diritto alla riservatezza del candidato e del lavoratore (la definizione, infatti, riguarda ambedue i soggetti) poiché in un momento storico in cui il progresso tecnologico non aveva ancora raggiunto l'attuale grado di sviluppo, cercava di proteggere la sfera privata del lavoratore, ponendosi l'obiettivo di fornire soluzione ad un problema che solo successivamente avrebbe raggiunto il suo apice. Il diritto alla riservatezza di cui allo Statuto dei lavoratori, infatti, non coincide ancora con la moderna idea di *privacy*. Più in particolare per comprendere tale evoluzione occorre osservare che gli interpreti civilisti, negli ultimi decenni, abbiano affermato che l'identità del singolo è il portato di scelte quotidiane che ne svelano i singoli aspetti che si traducono inevitabilmente in informazioni personali potenzialmente suscettibili di entrare nel dominio di terzi mediante le sempre più sviluppate tecnologie informatiche ([39]). Da qui ne discende che il termine riservatezza si sia arricchito di un ulteriore caratteristica, vale a dire il diritto a mantenere il

([39]) A. CATAUDELLA, *Art. 8* in U. PROSPERETTI, (diretto da), *Commentario dello Statuto dei lavoratori*, Milano, Giuffrè, 1975.

controllo sui dati personali coinvolti in flussi circolatori, e quindi nel diritto ad essere proprietari dei dati che ci appartengono ([40]).

Tornando alla formulazione dell'art. 8 bisogna distinguere una prima parte, che pone un divieto assoluto di indagine da parte del datore di lavoro sulle informazioni che riguardano l'orientamento ideologico del lavoratore (opinioni politiche, religiose o sindacali) che, per il legislatore, sono sempre ritenute estranee ed ininfluenti per valutare la prestazione lavorativa. Mentre, nella seconda parte emerge che le indagini effettuabili legittimamente dal datore di lavoro sono solo quelle "rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore", ossia che abbiano un'immediata e diretta correlazione con le mansioni dedotte e deducibili nel contratto di lavoro.

La realtà empirica di cui si è occupata la giurisprudenza negli anni successivi all'emanazione dello Statuto ha concretizzato ed esteso il dettato di cui all'art. 8 considerando, a mero titolo esemplificativo, vietate le indagini anche sulla posizione militare del lavoratore ([41]), sullo stato di gravidanza ([42]), sui vincoli di coniugio o di parentela ([43]), sulla residenza del prestatore ([44]).

([40]) E. STENICO, *Il trattamento dei dati personali del lavoratore subordinato: dalla segretezza al controllo*, in *Quaderni di diritto del lavoro e relazioni industriali*, Milano, UTET, n. 24, 2000.
([41]) Pretura Milano, 27/2/1975, in *Rivista Italiana di Diritto del Lavoro*, Milano, Giuffrè, II, 882, 1975.
([42]) Pretura Milano, 10/12/1974, in *Rivista Italiana di Diritto del Lavoro*, Milano, Giuffrè, II, 236, 1977.
([43]) Cass. 19/1/2002, n. 570, in *Rivista Italiana di Diritto del Lavoro*, Milano, Giuffrè, 511, 2002.
([44]) Cass. 28/3/1984, n. 2052, in *Foro italiano,* 1984.

2.1.2. I controlli a distanza

L'art. 23 del d.lgs. n. 151/2015 prima, e successivamente l'art. 5 comma 2 del d.lgs. n.185/2016 nell'ambito della riforma denominata *Jobs Act*, hanno riformato la disciplina dei controlli a distanza del lavoratore (e non anche del candidato) contenuta nello Statuto, per rimediare alla obsolescenza della norma del 1970, modificando l'art. 4 dello Statuto nella seguente attuale formulazione ([45]):

"1. Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, della sede centrale dell'Ispettorato nazionale del lavoro. I provvedimenti di cui al terzo periodo sono definitivi.

([45]) M. BARBIERI, *L'utilizzabilità delle informazioni raccolte: il Grande Fratello può attendere (forse)*, in P. TULLINI, (a cura di) *Controlli a distanza e tutela dei dati personali del lavoratore*, Torino, Giappichelli, 2017.

2. La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.

3. Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili 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 decreto legislativo 30 giugno 2003, n. 196."

La legge delega, che precedeva i predetti decreti legislativi ha previsto la "revisione della disciplina dei controlli a distanza sugli impianti e sugli strumenti di lavoro, tenendo conto dell'evoluzione tecnologica e contemperando le esigenze produttive ed organizzative dell'impresa con la tutela della dignità e della riservatezza del lavoratore" (Legge delega 10/2014, n.183, art.1, comma 7, lettera. f).

La precedente versione dell'art. 4, come concepita dal legislatore del 1970, conteneva un divieto assoluto di controllo a distanza dell'attività dei lavoratori (comma 1), permettendo però l'installazione di strumenti in grado di consentire tali controlli in presenza di esigenze organizzative e produttive e previo accordo sindacale o autorizzazione amministrativa (comma 2).

La norma, ben presto, dimostrò di non reggere più il passo dell'innovazione tecnologica, e un intervento del legislatore si ritenne necessario per tre principali motivi ([46]).

Il primo fu che nella precedente versione non erano conosciuti gli strumenti multifunzione, ossia strumenti di lavoro che consentissero, sia pur accidentalmente, il controllo a distanza dei lavoratori; tra questi rientrano ad esempio, il *computer*, i *tablet*, lo *smartphone*, il *telepass*, la carta di credito

([46]) I. ALVINO, *L'art. 4 dello Statuto dei lavoratori alla prova di internet e della posta elettronica*, in *Diritto delle relazioni industriali*, Milano, Giuffrè, 4/2014.

aziendale, i *badge*, tutti strumenti con una funzionalità inevitabilmente mista lavoro-controllo.

La mancanza di flessibilità del legislatore del 1970, che non conosceva tutta la strumentazione tecnologica che successivamente si sarebbe utilizzata nel mondo del lavoro, si traduceva nel paradosso per cui il datore di lavoro avrebbe dovuto sottoporre alle procedure di autorizzazione preventive all'installazione una quantità enorme di strumenti, quali quelli sopra ricordati.

Il secondo motivo di riforma era legato alla necessità di risolvere il contrasto giurisprudenziale formatosi sui c.d. controlli difensivi, che aveva individuato una zona franca rispetto all'applicazione della norma. Il controllo, infatti, veniva definito "difensivo" allorché il datore di lavoro aveva lo scopo di accertare un illecito commesso dal lavoratore e più in generale per finalità di tutela del patrimonio aziendale. Secondo questo primo orientamento, in tale circostanza il controllo non rientrerebbe nell'ambito dell'art. 4 dello Statuto, poiché l'oggetto del controllo non sarebbe una prestazione lavorativa, bensì una condotta illecita, diversa dal controllo vietato dalla norma ([47]).

Si formò, peraltro, un orientamento contrario in giurisprudenza, secondo il quale "l'esigenza, pur meritevole di tutela, del datore di lavoro di evitare condotte illecite da parte dei dipendenti non può assumere una portata tale da giustificare un sostanziale annullamento di ogni forma di garanzia della dignità e riservatezza del lavoratore" ([48]). Tale contrasto si risolverà parzialmente con la nuova formulazione dell'art. 4.

Terzo ed ultimo motivo era la necessità di un più opportuno coordinamento con la normativa generale sul trattamento dei dati personali, considerata l'entrata in vigore del Codice privacy (d.lgs. n.196/2003) ed i

([47]) A. BELLAVISTA, *Il controllo sui lavoratori*, Torino, Giappichelli, 1995.
([48]) Cass. 17/7/2007 n. 15892 in *Rivista Italiana di Diritto del Lavoro*, Milano, Giuffrè, 714, 2008, con nota di M. VALLURI.

provvedimenti del Garante privacy (ad esempio, Linee Guida del 1/3/2007 sul trattamento di dati mediante Internet e posta elettronica aziendale).

Il primo intervento rilevante della nuova formulazione dell'art. 4 sopra richiamata è stato finalizzato a semplificare l'installazione e l'utilizzo di quegli strumenti per i quali non opera l'obbligo di preventivo accordo sindacale o autorizzazione amministrativa. Si tratta degli strumenti "utilizzati dal lavoratore per rendere la prestazione lavorativa" e quelli "di registrazione degli accessi e delle presenze".

Il secondo intervento è quello relativo ai c.d. controlli difensivi, sintetizzabile nell'inserimento della tutela del "patrimonio aziendale" tra le esigenze aziendali qualificate che legittimano l'impego di strumenti di controllo. La dottrina si è, peraltro, divisa sulla sopravvivenza o meno dei controlli difensivi a valle della riforma del *Jobs Act* tra chi ritiene che i controlli difensivi siano ormai assorbiti nella nuova regolamentazione, e pertanto consentiti tramite impianti autorizzati; e chi invece propone la sopravvivenza del concetto di controllo a distanza proponendone un aggiornamento in deroga all'art. 4 dello Statuto ([49]). Sulla questione dei controlli difensivi, anche a seguito della riforma del 2015, la questione rimane aperta.

Il terzo ed ultimo intervento consiste in un espresso richiamo (art. 4 comma 3) alla normativa sul trattamento dei dati personali vigente all'epoca della riforma, ossia il Codice privacy, condizionando i controlli a distanza ad una adeguata informazione fornita al lavoratore delle modalità d'uso degli strumenti e di effettuazione dei controlli ([50]).

([49]) M. MARAZZA, *I controlli a distanza del lavoratore di natura "difensiva"*, in P. TULLINI, *op. cit*.
([50]) L. CAIRO, U. VILLA*, I controlli a distanza a quattro anni dal Jobs Act*, in *Il lavoro nella giurisprudenza*, Milano, IPSOA, 7/2019.

2.2 Il trattamento dei dati dei lavoratori nel Regolamento generale per la protezione dei dati personali n. 2016/679 (GDPR).

Con riferimento al trattamento dei dati personali nell'ambito dei rapporti di lavoro, le due norme principali di riferimento sono l'art. 9 par. 2 lett. b) e l'art. 88.

La prima norma, già anticipata al paragrafo 1.4.2, riguarda un'eccezione specifica e puntuale al divieto di trattamento dei dati particolari, che riguarda tutti i casi in cui il trattamento è necessario per finalità connesse con la materia di diritto del lavoro, della sicurezza sociale e della protezione sociale. Tale trattamento dovrà essere autorizzato alternativamente o congiuntamente dal diritto dell'Unione, degli Stati membri, oppure dai contratti collettivi, qualora si sia in presenza di garanzie per i diritti fondamentali e per gli interessi del dipendente o di un soggetto avente diritto a prestazioni previdenziali o di assicurazione sociale, di cui vengono trattati i dati.

La norma dell'art. 88, al paragrafo 1 prevede che gli Stati membri possano adottare, con legge o tramite contratti collettivi, norme specifiche sul rapporto di lavoro volte ad assicurare la protezione dei diritti e delle libertà dei dipendenti, individuando una serie di ambiti in cui limitare il potere di controllo o di ingerenza del datore di lavoro sui dati dei lavoratori.

Nel paragrafo 2 il Regolamento sottolinea la necessità di adottare misure appropriate e specifiche a salvaguardia della dignità umana, degli interessi legittimi, e dei diritti fondamentali degli interessati in riferimento: - alla trasparenza del trattamento; - al trattamento dei dati personali nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune; - al monitoraggio sul posto di lavoro. In estrema sintesi, la scelta del legislatore europeo è stata quella di riservare ampia

discrezionalità agli Stati membri, sia pure all'interno dei limiti di cui ai principi riportati al secondo paragrafo e, inoltre, di assicurare continuità normativa in materia di tutele e prerogative del lavoratore e sindacali ([51]).

In merito alla necessità degli Stati membri di adottare misure specifiche va qui sottolineata l'importanza fornita dal Regolamento alla disciplina del consenso in ambito lavorativo, a cominciare dal considerando 155, che impone di prevedere le condizioni alle quali i dati personali nei rapporti di lavoro possono essere trattati sulla base del consenso del dipendente.

Si veda anche il considerando 42, nel quale, "il consenso non dovrebbe essere considerato liberamente espresso se l'interessato non è in grado di operare una scelta autenticamente libera o è nell'impossibilità di rifiutare o revocare il consenso senza subire pregiudizio". Il successivo considerando 43, poi, afferma che: "È opportuno che il consenso non costituisca un valido presupposto" per il trattamento "qualora esista un evidente squilibrio tra l'interessato e il titolare del trattamento". Si comprende, quindi, come la disciplina del consenso prevista dal Regolamento sia improntata alla massima prudenza, che deve essere la misura con cui gli Stati membri dovranno trattare la disciplina di settore, in particolare in ambito lavorativo.

Vi sono poi altre disposizioni nel GDPR relative al trattamento dei dati dei lavoratori, anche perché, a favore di questi ultimi, possono essere imputati tutti i diritti propri dell'"interessato" precisati nel Regolamento. Di seguito si ritiene utile riepilogarne alcuni tra i più significativi.

L'art. 15 ([52]), ad esempio, regola il diritto di accesso, volto a consentire al lavoratore di sapere dal datore di lavoro le informazioni trattate sul suo

([51]) A. MAZZARO, D. MAZZONE, *GDPR e rapporto di lavoro,* Milano, Giuffrè, 2020.
([52]) Art. 15 Reg. (UE) 27 aprile 2016, n. 679: "L' interessato ha il diritto di ottenere dal Titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso virgola di ottenere l'accesso ai dati personali [...]"

conto. Nell'art. 16 ([53]) il dipendente ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano, senza ingiustificato ritardo, nonché di ottenere l'integrazione dei dati personali incompleti.

In forza dell'art. 17 ([54]), poi, il lavoratore potrà avvalersi del "diritto all'oblio", chiedendo che, in presenza di dati personali che non siano più necessari per le finalità per le quali sono stati raccolti, vengano cancellati e non sottoposti a trattamento.

Un cenno merita l'art. 18, che prevede il diritto di limitazione del trattamento dei propri dati, nei casi in cui: il lavoratore contesti l'esattezza dei propri dati; il trattamento sia illecito; l'interessato si sia opposto adducendo motivi connessi alla sua situazione particolare ([55]).

Ancora, l'art. 30 ([56]), rivolto alle imprese che contano più di 250 dipendenti, richiede l'obbligatorietà di conservare un registro delle attività di trattamento dei dati personali.

L'art. 35 ([57]) prevede che si proceda a una valutazione d'impatto dei dati, qualora l'uso di nuove tecnologie presenti un elevato rischio per i diritti

([53]) Art. 16 Reg. (UE) 27 aprile 2016, n. 679: "L'interessato ha il diritto di ottenere dal Titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato hai diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa".

([54]) Art. 17 Reg. (UE) 27 aprile 2016, n. 679: "L' interessato ha il diritto di ottenere dal Titolare del trattamento la cancellazione di dati personali che lo riguardano senza ingiustificato ritardo e il Titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti [...]"

([55]) A. MONEA, *Trattamento dei dati lavorativi e protezione dei dati personali nell'ente locale*, in *Azienditalia*, Milano, IPSOA, 11/2018.

([56]) Art. 30 comma 5 Reg. (UE) 27 aprile 2016, n. 679: "Gli obblighi di cui ai paragrafi uno e due non si applicano alle imprese organizzazioni con meno di 250 dipendenti, a meno che il trattamento che si effettuano possa presentare un rischio per i diritti e le libertà dell' interessato, il trattamento non sia occasionale o includa il trattamento di categoria particolare di dati di cui all'articolo 9, paragrafo uno, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10".

([57]) Art. 35 comma 1 Reg. (UE) 27 aprile 2016, n. 679: "Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il

e le libertà delle persone fisiche, tra cui ovviamente sono ricompresi i lavoratori. I contenuti di questa valutazione sono anche puntualmente elencati nella descrizione dei trattamenti, nelle finalità degli stessi, e nelle misure individuate per fronteggiare gli eventuali rischi.

Infine, ai sensi dell'art. 37 viene individuato il Responsabile della Protezione dei Dati, che rappresenta una novità nel nostro Paese, le cui attività richiedono per la loro rilevanza il controllo puntuale dei lavoratori su larga scala ([58]).

contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi".

([58]) A. PIZZOFERRATO, *Gli effetti del GDPR sulla disciplina del trattamento aziendale dei dati del lavoratore*, in *Argomenti di Diritto del Lavoro*, Milano, La Tribuna, 4-5, 2018.

2.3 Il trattamento dei dati dei lavoratori nel Codice della Privacy come modificato dal D.lgs. 101 del 2018

Il Codice della privacy, a seguito delle modifiche introdotte dal d.lgs. n. 101/2018, disciplina il trattamento dei dati dei lavoratori nel Titolo VIII rubricato: "Trattamenti nell'ambito del rapporto di lavoro" (artt.111-116). Il decreto 101/2018, all'art. 22 comma 6, ha adeguato il Codice della privacy ai principi del GDPR in quanto compatibili, abrogando in buona parte la normativa previgente.

L'art. 111 ([59]) è stato modificato prevedendo la promozione, da parte del Garante, di regole deontologiche per le finalità di cui all'art. 88 del GDPR, nonché l'individuazione di specifiche modalità per le informazioni da rendere all'interessato. In effetti, la protezione dei dati personali, si fonda non soltanto sulle previsioni normative dell'Unione Europea e degli Stati membri, ma anche su un'applicazione uniforme di regole deontologiche, da intendersi come principi inerenti a specifici settori lavoristici o finalità di trattamento che prevedano misure ed accorgimenti a garanzia degli interessati ([60]). Il Codice della privacy affida al Garante la promozione di tale uniformità di regole, che confluiscono in Codici di deontologia nei diversi settori in ambito lavoristico.

L'art. 111-*bis* ([61]) tratta la materia dei *curricula* spontaneamente trasmessi al fine dell'instaurazione di un rapporto di lavoro. Il datore di lavoro

([59]) art. 111 D. Lgs. 30 giugno 2003, n. 196: "Il garante promuove, ai sensi dell'articolo 2 quater, l'adozione di regole deontologiche per i soggetti pubblici e privati interessati al trattamento dei dati personali effettuato nell'ambito del rapporto di lavoro per le finalità di cui all'articolo 88 del Regolamento, prevedendo anche specifiche modalità per le informazioni da rendere all' interessato".
([60]) M. MIRONE*, Il dato personale: cos'è e come trattarlo*, in M. MARTORANA, (a cura di) *GDPR e decreto legislativo 101/2018*, Padova, CEDAM, 2019
([61]) Art 111 – *bis* D. Lgs. 30 giugno 2003, n. 196: "Le informazioni di cui all'articolo 13 del regolamento, nei casi di ricezione dei curricula spontaneamente trasmessi dagli interessati al fine della instaurazione di un rapporto di lavoro, vengono fornite al momento

può trattare i dati personali del soggetto che ha spontaneamente inviato il curriculum, solo al momento del primo contatto utile, successivo all'invio del curriculum stesso. Il consenso al trattamento di tali dati non è dovuto.

La dottrina evidenzia come il legislatore abbia posticipato, e non già escluso, il consenso del trattamento in tal caso, considerato che il consenso evidentemente non può essere dato prima di ricevere l'informativa ([62]).

L'art. 113 conferma il divieto di indagine sulle opinioni del lavoratore, fornendo attualità e forza normativa all'art. 8 dello Statuto dei lavoratori e, inoltre, ribadisce la vigenza dell'art. 10 del d.lgs. n. 276/2003 relativo al "Divieto di indagini sulle opinioni e trattamenti discriminatori".

Si tratta del divieto previsto per le agenzie per il lavoro e per gli altri soggetti pubblici e privati autorizzati o accreditati, di trattare dati, di preselezionare i lavoratori o di effettuare qualsiasi indagine, anche con il consenso, in base a una serie di caratteristiche rilevanti della persona (ad esempio convinzioni personali, affiliazione sindacale o politica, credo religioso, orientamento sessuale, stato matrimoniale, stato di salute, ecc.), a meno che non si tratti di elementi che costituiscono un requisito essenziale dell'attività lavorativa o incidano sulle modalità di svolgimento della stessa. Un secondo divieto attiene al trattamento dei dati personali dei lavoratori che non siano attinenti al loro inserimento lavorativo e alle loro attitudini professionali.

Le predette proibizioni non impediscono comunque alle agenzie per il lavoro e agli altri soggetti pubblici e privati accreditati e autorizzati, di

---

del primo contatto utile, successivo all' invio del curriculum medesimo. Nei limiti delle finalità di quell'articolo 6, paragrafo 1, lettera b), del Regolamento, il consenso al trattamento dei dati personali presenti nei curricula non è dovuto.

([62]) L. BOLOGNINI, *Regole nazionali e deontologiche per trattamenti nell'ambito del rapporto di lavoro*, in L. BOLOGNINI, E. PELINO, *Codice privacy: tutte le novità del d.lgs. n. 101/2018*, Milano, Giuffrè, 2018.

assistere categorie di lavoratori c.d. svantaggiati nella ricerca di un'occupazione, e di fornire sevizi o azioni mirate agli stessi.

L'art. 114 ([63]) conferma quanto disposto dall'art. 4 dello Statuto dei lavoratori in merito alla possibilità dei controlli a distanza delle attività del lavoratore e l'adeguamento del Codice privacy al GDPR non comporta alcun cambiamento in materia, per cui i datori di lavoro possono continuare ad operare secondo le disposizioni dell'art. 4 così come modificate dal *Jobs Act*, anche per sanzionare disciplinarmente i dipendenti ([64]).

L'art. 115 ([65]) stabilisce che nell'ambito del rapporto di lavoro domestico, del telelavoro, e del lavoro agile, il datore di lavoro è tenuto a garantire al lavoratore il rispetto della sua personalità e della sua libertà morale. Inoltre, il lavoratore domestico è tenuto a mantenere la necessaria riservatezza per tutto quello che si riferisce alla vita familiare.

Per i lavoratori domestici va ricordato, che non si applica l'art. 4 dello Statuto dei lavoratori, trattandosi di un rapporto che non si effettua all'interno di un'impresa organizzata, bensì nell'ambito di un nucleo ristretto, di natura perlopiù familiare. Tuttavia, qualora venga installato un sistema di videosorveglianza in un'abitazione privata dove presta la sua attività un lavoratore domestico, occorre comunque fornire a quest' ultimo l'informativa di legge e chiedere allo stesso il consenso. Il lavoratore domestico conserva

([63]) Art. 114 D. Lgs. 30 giugno 2003, n. 196: "Resta fermo quanto disposto dall' art. 4 della legge 20 maggio 1970, n. 300".
([64]) R. SCHIAVONE, *Nuovo codice privacy e gestione del rapporto di lavoro,* in *Il lavoro nella giurisprudenza*, Milano, IPSOA, 2018.
([65]) Art. 115 D. Lgs. 30 giugno 2003, n. 196: "Nell'ambito del rapporto di lavoro domestico del telelavoro e del lavoro agile il datore di lavoro è tenuto a garantire al lavoratore il rispetto della sua personalità e della sua libertà morale. Il lavoratore domestico è tenuto a mantenere la necessaria riservatezza per tutto quanto si riferisce alla vita familiare".

ovviamente il diritto di revocare il proprio consenso, e la revoca dello stesso non pregiudica la liceità del trattamento effettuato precedentemente ([66]).

([66]) R. DEL PUNTA, F. SCARPELLI, *Artt. 111 e ss. del d.lgs. 30/6/2003 n. 196 in Codice commentato del lavoro, Ed. I*, Milano, IPSOA, 2019.

2.4 Il trattamento dei dati personali dei lavoratori nell'interpretazione del Garante della privacy italiano.

L'art. 21 del d.lgs. n. 101/2018 ha imposto al Garante della privacy di individuare, con un provvedimento di carattere generale, le prescrizioni contenute nelle autorizzazioni generali già adottate nel 2016 con particolare riferimento al trattamento delle categorie particolari di dati. Il Garante prima ha avviato il procedimento attraverso una consultazione pubblica ultimata a gennaio 2019 e successivamente, ha emanato il Provvedimento del 5/6/2019 n. 146, pubblicato in Gazzetta Ufficiale n. 176 del 29/7/2019 contenente "Prescrizioni relative al trattamento di categorie particolari di dati". La prima delle prescrizioni recepite dal Garante, in adeguamento al GDPR, è quella relativa al "trattamento di categorie particolari di dati nei rapporti di lavoro", che in considerazione della sua importanza si ritiene utile riepilogare, precisando che il provvedimento si applica indistintamente ai datori di lavoro pubblici e privati, e che in generale i provvedimenti del Garante hanno rappresentato nel tempo un'importante fonte di prescrizioni e garanzie che aiutano i titolari del trattamento a conformarsi ai principi e agli obblighi in materia di protezione dei dati, facendo affidamento sulle indicazioni autorevoli già delineate dal Garante stesso.

L'ambito di applicazione del provvedimento riguarda tutti coloro che a vario titolo effettuano trattamenti per finalità di instaurazione, gestione ed estinzione del rapporto di lavoro (ad esempio, agenzie per il lavoro, imprese, enti, associazioni, organismi che utilizzano prestazioni lavorative o che conferiscono incarichi professionali, rappresentanti dei lavoratori per la sicurezza, organizzazioni rappresentative di categorie di datori di lavoro, medici competenti in materia di salute e sicurezza sul lavoro).

Il novero dei **soggetti interessati** all'interno del provvedimento è ampio, e comprende in particolare, oltre ai lavoratori subordinati, candidati all'assunzione, consulenti e liberi professionisti, agenti, rappresentanti e mandatari, lavoratori autonomi, persone fisiche che ricoprono cariche sociali, terzi danneggiati dall'esercizio dell'attività lavorativa o professionale.

Il Garante limita poi, nel provvedimento, il trattamento dei dati nel rapporto di lavoro ad alcune **finalità**, ed in particolare: 1) per adempiere o per esigere l'adempimento di specifici obblighi o per eseguire specifici compiti previsti dalla normativa dell'Unione Europea, da leggi, da regolamenti o da contratti collettivi, ai fini della gestione del rapporto di lavoro, del riconoscimento di agevolazioni, dell'applicazione della normativa in materia di previdenza ed assistenza o in materia di igiene e sicurezza del lavoro; 2) per perseguire finalità di salvaguardia della vita o dell'incolumità fisica del lavoratore; 3) per far valere o difendere un diritto in sede giudiziaria o in sede amministrativa; 4) per adempiere ad obblighi derivanti da contratti di assicurazione finalizzati alla copertura dei rischi connessi alla responsabilità dei datori di lavoro in materia di salute e sicurezza; 5) per garantire le pari opportunità nel lavoro; 6) per perseguire obiettivi in materia di assistenza sindacale ai datori di lavoro.

Specifici **obblighi** gravano, poi, sulle imprese prima, durante e dopo l'assunzione dei soggetti interessati.

Prima dell'assunzione il Garante ribadisce che, fermo restando che non possono essere trattati i dati genetici neppure con il consenso dell'interessato, i dati personali possono essere trattati solo per scopi determinati e legittimi e soltanto nella misura in cui la raccolta è necessaria per instaurare il rapporto di lavoro. Tutto ciò che è superfluo ai fini della instaurazione di un rapporto di impiego non va richiesto e, se fornito, non va utilizzato. Mentre, nel corso del rapporto di lavoro, il provvedimento del Garante precisa limitazioni (ad esempio in caso di fruizioni di permessi in occasione di festività religiose) al

trattamento dei dati concernenti, in particolare, la convinzione religiosa o la partecipazione ad associazioni religiose o filosofiche, nonché le opinioni politiche o l'appartenenza sindacale e l'esercizio di funzioni pubbliche (ad esempio ai fini della fruizione di permessi o di periodi di aspettativa) ([67]).

Il Garante della privacy ha di recente emesso alcune rilevanti decisioni in ambito lavorativo, tra le quali in particolare, il Provvedimento del 1° febbraio 2018 ([68]) in cui ha ritenuto illecito il trattamento dei dati personali effettuato dalla società datrice di lavoro sugli account di posta elettronica aziendale dei dipendenti, in considerazione del fatto che quest'ultima non aveva informato i lavoratori che le *e-mail* scambiate nel corso dell'attività lavorativa, sarebbero state conservate all'interno dei server aziendali per tutta la durata del rapporto di lavoro; anche dopo la cessazione dello stesso. Il trattamento, così effettuato costituisce una violazione dei principi di liceità, necessità e proporzionalità, oltre che un contrasto con la disciplina in materia di controlli a distanza.

Con il provvedimento del 28 febbraio 2019 ([69]) è intervenuto in merito al trattamento dei dati personali dei dipendenti di una società di pulizia urbana effettuato mediante dispositivi indossabili. Nel caso di specie, la società aveva fornito a circa una settantina di dipendenti dei braccialetti elettronici dotati di GPS attraverso i quali la società si poneva come obiettivo quello di effettuare la lettura delle etichette elettroniche collocate sui cestini e di segnalare l'eventuale spostamento di quelli non ancora fissati al suolo. Obiettivo dichiarato della società era quello di rendicontare il lavoro dell'azienda attraverso uno strumento di controllo a distanza innovativo. Il Garante, sebbene abbia rilevato che il sistema fosse idoneo a consentire il

([67]) R. TUCCILLO, *Art. 9 Regolamento UE n. 2016/679 – Trattamento di categorie particolari di dati personali, op. cit*.
([68]) Garante per la Protezione dei Dati Personali, Provvedimento del 1° febbraio 2018, Doc. web n. 8018046
([69]) Garante per la Protezione dei Dati Personali, Provvedimento del 28 febbraio 2019, Doc. web n. 9094427

trattamento dei dati personali dei lavoratori, ha prescritto alla società di individuare una differente tipologia di dispositivo, che, anche per le sue caratteristiche esteriori, non sia lesiva della dignità dei lavoratori. In conclusione, nonostante non ci sia stato alcun provvedimento sanzionatorio, il l'Autorità Garante ha comunque obbligato la società a conformare il trattamento dei dati relativi ai dipendenti ai principi di protezione dei dati, nei termini da loro indicati.

Inoltre, con provvedimento del 9 gennaio 2020 ([70]). il Garante della privacy ha sanzionato la società Tim S.p.a. per aver utilizzato un sistema completo di funzionalità di geolocalizzazione installato su dispositivi *smartphone* affidato ai dipendenti che svolgono mansioni di tecnico. La sanzione imposta dal Garante è stata motivata dal fatto che la società in questione non aveva sempre reso visibile sullo schermo del dispositivo un'icona che indicasse che la funzionalità di localizzazione fosse attiva.

([70]) Garante per la Protezione dei Dati Personali, Provvedimento correttivo e sanzionatorio nei confronti di Tim S.p.A., 9 gennaio 2020, Doc. web n. 9263597.

2.5 Il trattamento dei dati personali dei lavoratori nell'interpretazione dei Garanti europei: l'opinion n. 2 del 2017 del Gruppo di lavoro Articolo 29.

In applicazione dei principi del GDPR nel rapporto di lavoro, un riferimento imprescindibile è rappresentato dal Gruppo di lavoro Articolo 29 per la protezione dei dati, istituito dall'art. 29 della direttiva 95/46/CE, che riuniva le Autorità Garanti dei diversi Stati membri. Si tratta di un organismo di fondamentale rilevanza in quanto organo consultivo indipendente dell'UE per la protezione dei dati personali e della vita privata e ha rappresentato il preludio dell'attuale Comitato dei Garanti Europei (*European Board*) che ha il compito di seguire la corretta applicazione del GDPR nei singoli Paesi ([71]).

Il Gruppo di lavoro Articolo 29 ha effettuato un importante studio ed approfondimento in tema di trattamento dei dati dei lavoratori con il parere n. 2 dell'8/6/2017,[72] di grande interesse, perché tiene conto sia del GDPR sia dell'evoluzione delle nuove procedure informatiche (ad esempio sistemi per il controllo di lavoro da remoto, geolocalizzazione, etc.).

Il parere si pone l'obiettivo di descrivere i rischi posti dalle nuove tecnologie, valutando la proporzionalità delle scelte degli operatori in un equilibrio tra gli interessi legittimi del datore di lavoro e le ragionevoli aspettative dei dipendenti in materia di tutela della vita privata. A tal fine descrive numerosi scenari di trattamento in ambito lavorativo, tipici di rischio per i diritti e le libertà fondamentali dei lavoratori ([73]):

([71]) G. PEDRAZZI, *Art. 88 Regolamento UE n. 2016/679 – Trattamento dei dati nell'ambito dei rapporti di lavoro*, in S. PAGLIANTINI, (a cura di), *op. cit*.
([72]) Gruppo di Lavoro Articolo 29 per la protezione dei dati, Parere 2 dell'8/6/2017 sul trattamento dei dati sul posto di lavoro, in www.privacy.it.
([73]) A. PIZZOFERRATO, *op. cit.*

- Il **primo scenario** riguarda il trattamento durante il processo di assunzione, nel corso del quale i datori di lavoro non dovrebbero supporre di essere autorizzati a trattare per le proprie finalità i dati del candidato sui *social media* per il fatto che il profilo del soggetto è pubblicamente accessibile. Mentre, per poter procedere a un simile trattamento deve disporre di un fondamento giuridico, ad esempio un legittimo interesse. Ed inoltre sarà autorizzato a raccogliere e trattare i dati del candidato solo nella misura in cui tale raccolta è necessaria e pertinente per l'esecuzione del lavoro per il quale è stata presentata domanda.

- Il **secondo scenario** riguarda il trattamento per effettuare attività di *screening* sui dipendenti durante il periodo di impiego, raccogliendo ad esempio informazioni che afferiscono alla vita privata e familiare dei dipendenti. Tali *screening* devono essere esclusi e il datore di lavoro si dovrà astenere dal chiedere al dipendente l'accesso alle informazioni sui social che questi condivide con altre persone. Il WP 29 propone poi un esempio dimostrativo di un'attività di *screening* lecita da parte del datore di lavoro, ossia quella del monitoraggio dei profili social utilizzati per finalità lavorativa (ad esempio *Linkedin*) di ex dipendenti per la durata dell'applicazione delle clausole di non concorrenza.

- Il **terzo scenario** riguarda i trattamenti a seguito di monitoraggio sull'uso di tecnologie dell'informazione sul posto di lavoro, (telefono, navigazione in internet, posta elettronica, messaggistica istantanea) vera minaccia per la riservatezza secondo il WP 29. Per limitare tale pericolo i Garanti incoraggiano i datori di lavoro ad adottare tutte quelle soluzioni utili a prevenire il ricorso ad accessi successivi ai dati dei lavoratori, come ad esempio una valutazione d'impatto del trattamento dei dati.

- Il **quarto scenario** è relativo al monitoraggio sull'uso delle tecnologie dell'informazione al di fuori del posto di lavoro. Tali trattamenti riguardano quelle situazioni, sempre più frequenti, relative al lavoro a domicilio, al

lavoro a distanza, e all'utilizzo dei propri dispositivi (*bring your own device*) nelle quali il datore di lavoro non può adottare misure di sicurezza sproporzionate ed eccessive rispetto alle finalità perseguite (in tal senso sarebbe da ritenersi, ad esempio, vietato il monitoraggio dei movimenti del *mouse,* l'utilizzo di *webcam* o di tecnologie di *screen capture*).

- Il **quinto scenario** si riferisce ai trattamenti effettuati utilizzando sistemi di monitoraggio video per controllare gli accessi presso le sedi aziendali e il tracciamento delle attività dei dipendenti.

Il WP 29 pone anche un esempio a riguardo, ossia il caso in cui il datore di lavoro installi in una sala server un sistema di controllo degli accessi che registra l'ingresso e l'uscita dei dipendenti che dispongono di una autorizzazione per accedere in tale ambiente. Il monitoraggio continuo della frequenza e degli orari precisi di entrata e di uscita dei dipendenti può essere effettuato solo in virtù di un legittimo interesse e purché i dipendenti ne siano adeguatamente informati. Mentre non può essere giustificato se tali dati vengono utilizzati per altre finalità, quali ad esempio la valutazione del rendimento dei dipendenti.

- Il **sesto scenario** riguarda il trattamento di dati personali sull'utilizzo dei sistemi di videosorveglianza, i quali per loro natura sono in grado di eccedere le limitazioni necessarie al trattamento dei dati dei lavoratori. Tipico è il caso dell'utilizzo di questi strumenti per il riconoscimento facciale, che invece dovrebbe ritenersi illecito in via di principio salvo non venga colmata la sproporzione del trattamento rispetto ai diritti e alle libertà del dipendente.

- Il **settimo scenario** riguarda i sistemi di geolocalizzazione sul veicolo utilizzato dal dipendente. Tali dati possono includere non solo la posizione del veicolo, ma anche il comportamento di guida del dipendente. Il WP 29 richiede che i datori di lavoro non debbano considerarli come strumenti per

seguire o monitorare il comportamento o gli spostamenti dei dipendenti, ad esempio inviando segnali di allarme in relazione alla velocità del veicolo.

- L'**ottavo scenario** riguarda le operazioni che implicano la divulgazione di dati dei dipendenti a terzi, come nel caso delle aziende che trasmettono i dati dei dipendenti ai clienti per garantire un servizio affidabile. Il rischio è che tali dati possano essere sovrabbondanti, tenuto conto che i dipendenti non sono in grado, dato lo squilibrio di potere, di dare libero consenso al trattamento dei dati personali.

- Il **nono e ultimo scenario** si occupa di trattamenti che comportano trasferimenti internazionali di dati relativi alle risorse umane e altri dati dei dipendenti. I Garanti precisano che il trasferimento deve ritenersi legittimamente adottato qualora il Paese terzo, al di fuori della UE, garantisca un livello di protezione adeguato ([74]).

([74]) A. MAZZARO, D. MAZZONE, *op. cit*.

CAPITOLO II

Il trattamento dei dati giudiziari nel rapporto di lavoro

SOMMARIO: 1. La nozione di dato giudiziario e i principi di trattamento. -2. Il trattamento dei dati giudiziari nel Regolamento UE 679/2016 e nel Codice della privacy: un vuoto da colmare - 3. Il trattamento dei dati giudiziari e normativa speciale: il settore bancario e assicurativo. - 4. Il trattamento dei dati giudiziari del lavoratore nella giurisprudenza nazionale antecedente al Regolamento UE 679/2016 e al D. Lgs 101/2018.

1. La nozione di dato giudiziario e i principi di trattamento

Il trattamento dei dati relativi a condanne penali, a reati o alle connesse misure di sicurezza costituisce senza dubbio uno degli ambiti più delicati della disciplina europea e nazionale a tutela dei dati personali. Si tratta, con ogni evidenza, di dati che attengono alla sfera personalissima dell'individuo e che, per tale motivo, vengono seguiti da una disciplina specifica considerato che i fatti contenuti in sentenze penali, ma anche gli atti penali in genere (ad es. atti prodotti nel corso delle indagini preliminari), sono particolarmente significativi, non soltanto ai fini della profilazione ([75]) dei dati personali, ma anche ai fini dell'analisi e della previsione dell'affidabilità e del comportamento della persona (specialmente nel rapporto di lavoro).

La nozione di trattamento di dati personali relativi a condanne penali e reati è contenuta nell'art. 10 del Regolamento UE 2016/679 che così dispone: "Il trattamento di dati personali relativi alle condanne penali e ai reati o alle connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo delle autorità pubblica o se il trattamento è autorizzato dal diritto dell' Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica".

Il criterio fondamentale che guida questa norma è che il trattamento dei dati giudiziari debba avvenire prioritariamente e come criterio generale sotto il controllo dell'autorità pubblica, salvo che il trattamento sia autorizzato dal

([75]) E. PELLECCHIA, *Profilazione e decisioni automatizzate al tempo della Black Box Society: qualità dei dati e eleggibilità dell'algoritmo nella cornice della responsabile research and innovation*, in *Nuove Leggi Civili Commentate*, Padova, CEDAM, 2018.

diritto degli Stati membri in base a una norma di legge in modo da prevedere garanzie appropriate per i diritti e le libertà degli interessati.

La significatività di tali dati appare ulteriormente confermata dai Considerando n. 97, 115 e 113 del GDPR i quali indicano rispettivamente che il trattamento dei dati relativi a condanne penali e reati debba avvenire con l'ausilio di persone adeguatamente competenti in materia di protezione dei dati (Considerando n. 97) ([76]), che potrebbero sorgere ostacoli alla protezione delle persone nel trasferimento di questo tipo di dati a Paesi terzi (Considerando n. 115) ([77]) e che per rendere più effettiva possibile la

([76]) Considerando 97 Reg. (UE) 27 aprile 2016, n. 679: "Per i trattamenti effettuati da un'autorità pubblica, eccettuate le autorità giurisdizionali o autorità giudiziarie indipendenti quando esercitano le loro funzioni giurisdizionali, o per i trattamenti effettuati nel settore privato da un titolare del trattamento le cui attività principali consistono in trattamenti che richiedono un monitoraggio regolare e sistematico degli interessati su larga scala, o ove le attività principali del titolare del trattamento o del responsabile del trattamento consistano nel trattamento su larga scala di categorie particolari di dati personali e di dati relativi alle condanne penali e ai reati, il titolare del trattamento o il responsabile del trattamento dovrebbe essere assistito da una persona che abbia una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati nel controllo del rispetto a livello interno del presente regolamento".

([3]) Considerando 115 Reg. (UE) 27 aprile 2016, n. 679: "Alcuni paesi terzi adottano leggi, regolamenti e altri atti normativi finalizzati a disciplinare direttamente le attività di trattamento di persone fisiche e giuridiche poste sotto la giurisdizione degli Stati membri. Essi possono includere le sentenze di autorità giurisdizionali o le decisioni di autorità amministrative di paesi terzi che dispongono il trasferimento o la comunicazione di dati personali da parte di un titolare del trattamento o di un responsabile del trattamento e non sono basate su un accordo internazionale in vigore tra il paese terzo richiedente e l'Unione o un suo Stato membro, ad esempio un trattato di mutua assistenza giudiziaria. L'applicazione extraterritoriale di tali leggi, regolamenti e altri atti normativi potrebbe essere contraria al diritto internazionale e ostacolare il conseguimento della protezione delle persone fisiche assicurata nell'Unione con il presente regolamento. I trasferimenti dovrebbero quindi essere consentiti solo se ricorrono le condizioni previste dal presente regolamento per i trasferimenti a paesi terzi".

([4]) Considerando 113 Reg. (UE) 27 aprile 2016, n. 679: "Potrebbero altresì essere autorizzati i trasferimenti qualificabili come non ripetitivi e riguardanti soltanto un numero limitato di interessati ai fini del perseguimento degli interessi legittimi cogenti del titolare del trattamento, a meno che non prevalgano gli interessi o i diritti e le libertà dell'interessato e qualora il titolare del trattamento abbia valutato tutte le circostanze relative al trasferimento. Il titolare del trattamento dovrebbe considerare con particolare attenzione la natura dei dati personali, la finalità e la durata del trattamento o dei trattamenti proposti, nonché la situazione nel paese d'origine, nel paese terzo e nel paese di destinazione finale, e dovrebbe offrire garanzie adeguate per la tutela dei diritti e delle libertà fondamentali delle persone fisiche con riguardo al trattamento dei loro dati personali. Tali trasferimenti dovrebbero essere

protezione delle persone dovrebbe essere incentivata la cooperazione dell'Unione europea con i Paesi terzi (Considerando n. 113) ([78]).

Può essere utile ora una breve analisi della disciplina previgente al Regolamento su tale materia per comprendere meglio come si è giunti alla attuale nozione. Già la direttiva 95/46/CE e la relativa disciplina nazionale di recepimento avevano definito un quadro di regole per il trattamento dei dati giudiziari.

L'art. 27 del d.lgs. n. 196/2003 (Codice privacy), consentiva il trattamento dei dati giudiziari da parte dei privati o di enti pubblici economici soltanto se autorizzato da espressa disposizione di legge o provvedimento del Garante che specificasse le rilevanti finalità di interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili. Il Garante della privacy si adeguò a tale disposizione con l'autorizzazione generale n. 7/2016, finalizzata specificatamente al trattamento di dati giudiziari da parte di privati, di enti pubblici economici e di soggetti pubblici ([79]), indicando una serie di ambiti nei quali il trattamento dei dati giudiziari era ritenuto legittimo, tra i quali il rapporto di lavoro e le imprese bancarie ed assicurative. Va ricordato, che in tale autorizzazione, l'Autorità Garante già prevedeva che nell'ambito dei rapporti di lavoro l'autorizzazione al trattamento dei dati giudiziari era rilasciata alle associazioni e agli organismi che facessero parte di un rapporto di lavoro, e che il trattamento dei dati giudiziari era indispensabile per adempiere ai contratti collettivi di lavoro, anche aziendali.

Pertanto, si può affermare in linea generale, che prima dell'entrata in vigore del GDPR la modalità principale di autorizzazione al trattamento dei

---

ammessi soltanto nei casi residui in cui nessuno degli altri presupposti per il trasferimento è applicabile.

([5]) Garante per la Protezione dei Dati Personali, Autorizzazione n. 7/2016 al Trattamento di dati giudiziari da parte di privati, di enti pubblici economici e di soggetti pubblici, in *Gazzetta Ufficiale* n. 303 del 29/12/2016.

dati giudiziari fosse la norma di legge ovvero il provvedimento del Garante ([80]).

A seguito dell'entrata in vigore del Regolamento il legislatore nazionale ha adeguato la normativa interna con il d.lgs. n. 101/2018 (abrogando anche, tra gli altri, l'art. 27 sopra richiamato) che ha introdotto nel Codice della privacy, l'art. 2 – *octies* recante i "Principi relativi al trattamento di dati relativi a condanne penali e reati".

I principi attualmente in vigore in merito al trattamento dei dati giudiziari sono pertanto quelli che, di seguito, andiamo ad esaminare.

1) **il primo** riguarda l'autorizzazione al trattamento dei dati giudiziari che, ribadendo quanto previsto dal GDPR, è consentita solo se autorizzata da una norma di legge o di regolamento che prevedano garanzie appropriate per i diritti e le libertà degli interessati. Viene fatto salvo quanto previsto dal d.lgs. 18/6/2018 n. 51, attuativo della direttiva 2016/680/UE ([81]), che contiene la disciplina relativa al trattamento dei dati giudiziari da parte delle autorità competenti di pubblica sicurezza ai fini di prevenzione, indagine, accertamento e perseguimento dei dati.

2) **Il secondo** principio sancisce che, in assenza di disposizioni di legge o di regolamento, i trattamenti dei dati giudiziari sono individuati con decreto del Ministro della Giustizia da adottarsi sentito il Garante.

3) **Il terzo** definisce in particolare gli ambiti nei quali la legge o il decreto del Ministro della Giustizia dovranno operare. Si ritiene che, per quanto riguarda tali ambiti, ispirati alla autorizzazione generale n. 7/2016 del

([80]) F. BIANCA, *Art. 10 Regolamento UE n. 2016/679 – Trattamento di dati personali relativi a condanne penali e reati*, in A. BARBA, S. PAGLIANTINI, (a cura di), *Commentario del codice civile – Delle persone – Leggi collegate Vol. II*, Milano, UTET Giuridica, 2019.
([81]) Si tratta della Direttiva sulla tutela dei dati personali usati dalla polizia e dalle autorità di giustizia penale pubblicata in Gazzetta Ufficiale dell'Unione europea il 4/5/2016.

Garante, si tratti di un elenco esemplificativo e non esaustivo ([82]). In estrema sintesi riguardano: i rapporti di lavoro; la mediazione finalizzata alla conciliazione delle controversie civili e commerciali; l'accertamento dei requisiti di onorabilità; l'attività assicurativa; l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria; il diritto di accesso agli atti amministrativi; l'esecuzione di investigazioni o ricerche di pubblica sicurezza; l'adempimento di obblighi in materia di disposizioni antimafia nonché l'accertamento del requisito di idoneità morale per partecipare a gare d'appalto; la disciplina in materia di attribuzione del rating di legalità delle imprese; le attività di prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo.

4) **Il quarto** principio impone al decreto del Ministro della Giustizia di individuare le garanzie appropriate per i diritti e le libertà degli interessati.

5) **Il quinto** principio riguarda l'eventualità che il trattamento dei dati avvenga sotto il controllo dell'autorità pubblica, e in tal caso si applicano le garanzie previste dall'art. 2 – *sexies* per i motivi di interesse pubblico rilevante

6) **Il sesto** principio prevede che con il decreto del Ministro della Giustizia possano essere autorizzati i trattamenti dei dati giudiziari effettuati in attuazione dei protocolli di intesa per la prevenzione e il contrasto dei fenomeni di criminalità organizzata stipulati in accordo con il Ministero dell'Interno e con le prefetture.

([82]) ASSONIME, nota n. 9 del 17/3/2020 – *Trattamento dei dati relativi a condanne penali e reati da parte delle imprese: verso l'attuazione dell'art. 2 - octies del Codice privacy* in www.assonime.it.

2. Il trattamento dei dati giudiziari nel Regolamento UE 679/2016 e nel Codice della privacy: un vuoto da colmare

Va analizzata adesso una questione di fondamentale importanza nel trattamento dei dati giudiziari, ossia il vuoto normativo che si è venuto a creare, a seguito del d. lgs. 101/2018, attuativo del GDPR. Infatti, ad oggi manca una legge, un regolamento o un decreto del Ministro della Giustizia necessari ad autorizzare e disciplinare (ai sensi dell'art. 2 - *octies* del d.lgs. n. 196/2003 così come modificato dal d.lgs. n. 101/2018) il trattamento dei dati giudiziari, con evidenti problematiche in merito alla possibilità di effettuare una serie di trattamenti assolutamente necessari per il normale svolgimento delle attività professionali, imprenditoriali e istituzionali.

Occorre, a questo punto, ricostruire i tratti salienti della vicenda. Come sopra richiamato il vecchio regime del Codice privacy prevedeva (all'art. 27 del d.lgs. 196/2003) che il trattamento dei dati giudiziari fosse consentito, oltre che da una legge, da un provvedimento del Garante. Il testo di riferimento era l'Autorizzazione generale n. 7/2016 al trattamento dei dati a carattere giudiziario da parte di privati, di enti pubblici economici e di soggetti pubblici.

Successivamente, prima il GDPR e poi il Codice privacy modificato dal d.lgs. 101/2018, all'art. 2 – *octies,* hanno introdotto un nuovo regime rafforzando la disciplina del trattamento dei dati giudiziari, lasciando al Garante solamente la funzione di emanare un parere sul decreto del Ministro della Giustizia.

Pertanto, l'efficacia dell'autorizzazione generale del Garante n. 7/2016, che fino a quel momento era stato lo strumento fondamentale previsto dall'ordinamento in tema di autorizzazione al trattamento dei dati giudiziari da parte di tutti i soggetti privati o pubblici, cessava, sulla base di quanto lo

stesso provvedimento dichiarava, al 25 maggio 2018 (data di entrata in vigore del GDPR). Con il Provvedimento del 19/7/2018, il Garante ([83]), in un'ottica di continuità e certezza del quadro normativo disponeva una proroga della vigenza delle autorizzazioni precedenti, consentendo la temporanea prosecuzione dei trattamenti dei dati giudiziari già autorizzati, fino all'entrata in vigore del decreto legislativo attuativo del GDPR, che sarebbe stato approvato il mese successivo.

Il 10 agosto 2018 veniva infatti approvato il d.lgs. 101/2018 che all'art. 21 comma 3 prescrive che le autorizzazioni generali del Garante cessano di produrre effetti alla sua entrata in vigore.

Incredibilmente, ad oggi, la problematica del vuoto normativo, ovvero della mancanza di una legge, di un regolamento e di un decreto del Ministro della Giustizia necessari ad autorizzare e disciplinare il trattamento dei dati giudiziari, non è stata ancora risolta, nonostante sia passato un triennio dal recepimento del GDPR nel nostro Paese.

Si cercherà di analizzare ora le possibili soluzioni ermeneutiche che, nel settore lavorativo, sono state offerte dagli interpreti per tentare di colmare il vuoto che si è determinato in materia.

Possono proporsi diverse soluzioni per tentare di sopperire alla mancanza di un adeguato intervento attuativo del legislatore o del Governo, che si riscontra in vari settori, e in particolar modo nel rapporto di lavoro, anche se occorre subito dire che nulla osta alla raccolta dei dati giudiziari nella Pubblica Amministrazione e nel lavoro a contatto con i minori dove già sono previste, in via eccezionale, norme di legge autorizzative al trattamento dei dati giudiziari.

([83]) Garante per la Protezione dei Dati Personali, Provvedimento del 19/7/2018 in tema di Autorizzazioni generali del Garante per la protezione dei dati personali, Doc. web n. 9026901.

Infatti, nella Pubblica Amministrazione il fondamento giuridico è dato dal d.p.r. 487/1994 che all'art. 2 comma 3 prevede che "Non possono accedere agli impieghi coloro che siano esclusi dall'elettorato politico attivo e coloro che siano stati destituiti o dispensati dall'impiego presso una pubblica amministrazione". Tale norma si estende anche ai contratti di formazione e lavoro nonché ai contratti di somministrazione di lavoro a tempo determinato (art. 36 d.lgs. 165/2001). In ragione di tale disposizione si desume una base di autorizzazione al trattamento dei dati giudiziari nella fase di partecipazione al concorso e nel corso dello svolgimento del rapporto con la Pubblica Amministrazione.

Quando si tratti di un lavoro a contatto con minori, opera invece l'art. 2 del d.lgs. n. 39/2014 secondo il quale i soggetti che intendono impiegare una persona per lo svolgimento di attività professionali o attività volontarie organizzate che comportino contatti diretti e regolari con minori devono richiedere il certificato penale del casellario giudiziale ([84]) (c.d. certificato antipedofilia) ([85]).

Si ritiene ora necessario individuare quali siano gli orientamenti sviluppatisi per tentare di fornire, in via generale e al di là delle eccezioni appena viste, una risposta al vuoto esistente nella disciplina sul trattamento dei dati giudiziari nel rapporto di lavoro privato in attesa che siano varati i prescritti provvedimenti autorizzativi, senza la pretesa di fornire una soluzione esaustiva, che non potrà che avvenire con l'approvazione del decreto del Ministro della Giustizia.

([84]) Il testo unico in materia di casellario giudiziale è stato approvato con il D.p.r 14/11/2002 n. 313, integrato dal D.Lgs. 2/10/2018 n. 122 (c.d. riforma Orlando). Sulla base di tale norma nel certificato penale del casellario giudiziale risultano i "provvedimenti giudiziari penali di condanna definitivi".
([85]) R. DEL PUNTA, F. SCARPELLI, (a cura di) *Art. 2 – octies del Codice in materia di dati personali* in *op. cit*.

Una prima risposta al vuoto esistente potrebbe essere quella di ritenere di essere autorizzati comunque al trattamento di dati giudiziari ai sensi dell'art. 8 dello Statuto dei lavoratori che, come ricordato nel capitolo precedente, afferma l'esistenza di un divieto di indagini su fatti "non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore". Il trattamento del dato giudiziario, per converso, qualora fosse rilevante nella valutazione dell'attitudine lavorativa del dipendente e quindi coerente con le mansioni svolte, e la raccolta dei dati fosse necessaria e pertinente, sarebbe consentito sulla base di un'interpretazione estensiva dell'art. 8.

Ad avviso di chi scrive, far risalire all'art. 8 dello Statuto dei lavoratori (che impone un divieto normativo) un'autorizzazione generale al trattamento dei dati giudiziari, appare soluzione poco convincente dal punto di vista giuridico, tanto più in considerazione della delicatezza dei dati in questione.

Una seconda soluzione teorica sarebbe quella di conservare le misure previste dalla Autorizzazione Generale n. 7/2016, attribuendole una sorta di ultrattività nell'attesa dei futuri provvedimenti (che è ragionevole pensare non se ne discosteranno sensibilmente sul piano sostanziale) ([86]).

Un'altra soluzione ipotizzata sarebbe quella di richiedere un'autocertificazione ai sensi del d.p.r. n. 445/2000, prassi in uso in alcune organizzazioni private, in cui il lavoratore dichiara di non avere condanne o procedimenti penali in corso ([87]). La soluzione prospettata sembra difficile da immaginare, data la dubbia utilizzabilità di una dichiarazione di natura amministrativa in ambito privatistico per il trattamento dei dati giudiziari, che

([86]) F. BIANCA, *op cit*. in cui l'autore afferma che il trattamento dei dati relativi a condanne penali in assenza del decreto del Ministro competente, possa essere svolto sotto il controllo dell'autorità pubblica designata dalla legge ad esercitare il controllo sull'attività di trattamento, che continua ad essere il Garante per la protezione dei dati personali.
([87]) Va sottolineato che con il d.lgs. 2/10/2018 n. 122 (c.d. riforma Orlando), si è proceduto alla riforma del casellario giudiziale, ed è stato risolto il problema di quali precedenti penali dichiarare in un'autocertificazione, non essendo più l'interessato tenuto a dichiarare determinate condanne o specifici provvedimenti di lieve o minore entità.

sono per loro natura materia di elevata sensibilità, ma anche a prescindere dalla natura amministrativa dell'autocertificazione saremmo sempre in presenza di un trattamento di dati giudiziari per mezzo dell'autocertificazione stessa, non autorizzato ([88]).

Infine, vi è chi, come Assonime ([89]), fornisce alcune indicazioni utili per l'emanando decreto del Ministro della Giustizia, la cui entrata in vigore ritiene essere necessaria ai fini dell'autorizzazione normativa al trattamento dei dati giudiziari nel rapporto di lavoro, riconoscendo che una base rilevante è fornita dall'Autorizzazione Generale n. 7/2016 ([90]).

A tal fine, l'Assonime fornisce una serie di suggerimenti al Governo. Innanzitutto, il decreto ministeriale per i rapporti di lavoro dovrebbe prevedere che il **trattamento sia autorizzato** per l'adempimento degli obblighi e l'esercizio dei diritti da parte del titolare e dell'interessato. Inoltre, il decreto autorizzativo dovrebbe precisare **quali siano i soggetti che possono effettuare il trattamento dei dati** ed in particolare le persone fisiche e giuridiche, gli enti, le associazioni e gli organismi che oltre a essere parte di un rapporto di lavoro, utilizzano prestazioni lavorative atipiche, parziali o temporanee, ovvero conferiscono un incarico professionale a consulenti, liberi professionisti, agenti, rappresentanti o mandatari.

Successivamente, sempre in linea con l'Autorizzazione Generale n. 7/2016, il decreto dovrebbe specificare che il **trattamento può riguardare soggetti** che hanno assunto o intendano assumere la qualità di: lavoratori

([88]) R. MARAGLINO, *Dati giudiziari, fermo al palo il trattamento per i lavoratori*, in www.agendadigitale.eu, 31/10/2019.
([89]) Assonime è l'associazione tra le società italiane per azioni, costituitasi nel 1910. L'associazione si occupa prevalentemente di imposizione fiscale diretta e indiretta, diritto societario, mercato dei capitali e società quotate, attività di impresa e concorrenza. Si tratta si un laboratorio intellettuale che interpreta le leggi con un approccio *pro veritate*, fornisce chiarimenti alle sue associate e offre analisi su materie tecniche.
([90]) ASSONIME, nota n. 9 del 17/3/2020, *op. cit*.

subordinati, consulenti, liberi professionisti, agenti, rappresentanti e mandatari.

Infine, i datori di lavoro, dovrebbero adottare un **criterio adeguato alla conservazione dei dati**, che tenga conto di alcuni requisiti minimi quali ad esempio: l'accesso ad essi solo a personale autorizzato, una durata di trattamento limitata alla effettiva necessità di detenzione del dato, la conservazione in ambienti sicuri, la distruzione dei dati non più necessari.

In conclusione, finché non interverrà il decreto ministeriale sopra richiamato o siano rintracciate norme di legge o regolamenti che autorizzino il trattamento dei dati giudiziari, l'acquisizione di tali dati è in contrasto con l'ordinamento interno e con quello comunitario anche qualora sia ammesso da una specifica previsione del contratto collettivo. Peraltro, dopo critiche e sollecitazioni intervenute da più parti, la pubblicazione del decreto del Ministro della Giustizia dovrebbe arrivare a breve, richiamando, a grandi linee, l'impostazione seguita dal Garante della privacy nei suoi precedenti provvedimenti: autorizzando il trattamento dei dati giudiziari sulla base di una previsione del contratto collettivo.

In attesa della auspicata adozione del decreto del Ministro della Giustizia, i datori di lavoro dovranno agire responsabilmente entro il perimetro dell'art. 2 - *octies* del Codice privacy per evitare il rischio di effettuare un trattamento non necessario e non proporzionato attraverso interpretazioni forzatamente estensive di altre previsioni normative. Inoltre si potrebbe addirittura integrare il reato di trattamento illecito disciplinato dall'art. 167 ([91]) del D. Lgs 196 del 2003, in caso di violazione dell'art. 2 – *octies* del codice privacy.

([91]) Art. 167 D. Lgs. 196/2003: "Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trattamento dei dati personali di cui agli articoli 9 e 10 del Regolamento in violazione delle disposizioni di cui agli articoli 2 – *sexies* e 2 – octies, o delle misure di garanzia di cui all'art. 2 – sexies ovvero operando in violazione delle misure adottate ai sensi dell'art. 2 –

quinquiesdecies arreca nocumento all'interessato, è punito con la reclusione da uno a tre anni".

3. Il trattamento dei dati giudiziari e normativa speciale: il settore bancario e assicurativo

Vi sono però alcuni settori in cui i datori di lavoro possono vantare una specifica previsione di legge o un decreto ministeriale emanato ai sensi di legge che consenta loro di trattare i dati giudiziari dei loro interlocutori.

Si tratta del settore bancario e del settore assicurativo, ambedue dotati di specifiche norme, contenute rispettivamente nel Testo Unico Bancario e nel Codice delle assicurazioni private, che prevedono garanzie appropriate per i diritti e libertà degli interessati, rispetto ai quali i datori di lavoro trattano i dati giudiziari.

Per quanto riguarda il **settore bancario**, opera l'art. 26 del d.lgs. 385/1993 del TUB (Testo Unico Bancario), come modificato dal d.lgs. 12/5/2015, n. 72, che ha recepito nel nostro ordinamento la Direttiva 2013/36/UE (*Capital Requirements Directive*, nota come CRD IV) ([92]).

La norma attribuisce al Ministro dell'economia e delle finanze il compito di individuare, con decreto adottato sentita la Banca d'Italia, i requisiti e i criteri di idoneità che devono soddisfare gli esponenti aziendali delle banche, i limiti al cumulo degli incarichi che possono essere ricoperti dagli stessi, le cause che comportano la sospensione temporanea della carica e la loro durata, i casi in cui requisiti e criteri di idoneità si applicano anche ai responsabili delle principali funzioni aziendali nelle banche di maggiore dimensione e complessità operativa.

Dopo due anni dall'avvio di un'apposita consultazione da parte del Ministero dell'economia e delle finanze (MEF) dello schema di decreto, il

([92]) Direttiva 2013/36/UE del Parlamento europeo e del Consiglio del 26/6/2013, in *Gazzetta Ufficiale dell'Unione Europea*, 27/6/2013.

15/12/2020 è stato pubblicato nella Gazzetta Ufficiale il decreto del MEF n. 169 del 23/11/2020 recante disposizioni regolamentari in materia di requisiti e criteri di idoneità per lo svolgimento dell'incarico degli esponenti delle banche e degli intermediari finanziari. Detto provvedimento è entrato in vigore il 30 dicembre 2020 e le disposizioni ivi contenute trovano applicazione alle nomine successive alla suddetta data ([93]).

Il decreto si sofferma in particolare sui dati giudiziari degli esponenti aziendali (sentenze definitive e non, indagini e procedimenti penali in corso, irrogazioni di sanzioni amministrative, provvedimenti disciplinari quali la radiazione o la sospensione da albi professionali, ecc.) che, qualora accertati, comportano il venir meno dei requisiti di onorabilità, correttezza e professionalità.

Si riepilogano di seguito le principali novità introdotte dal recente decreto ministeriale.

L'art. 2 attiene all'**ambito di applicazione** e individua i soggetti destinatari del provvedimento, ossia i componenti del consiglio di amministrazione, del consiglio di sorveglianza, del consiglio di gestione, i membri del collegio sindacale e i responsabili delle principali funzioni aziendali delle banche di maggiori dimensione o complessità operativa (vale a dire i responsabili delle funzioni antiriciclaggio, *compliance*, controllo dei rischi e revisione interna, il *chief financial officer*, nonché ove presente e se diverso da quest'ultimo, il dirigente preposto alla redazione dei documenti contabili societari).

All'art. 3 vengono definiti i **requisiti di onorabilità** degli esponenti aziendali, confermando la disciplina previgente contenuta nel Decreto del Ministro dell'Economia n. 161 del 1998, ampliando però la categoria dei reati

([93]) A. PEZZUTO, *Nuovi requisiti e criteri di idoneità degli esponenti aziendali*, in *Rivista di diritto bancario e finanziario Tidona*, www.tidona.com, 12/1/2021.

che, qualora accertati con sentenza definitiva, comportino il venir meno di tale requisito (ad esempio, si aggiungono reati previsti dalle disposizioni in materia di antiriciclaggio).

L'art. 4 contiene i **requisiti di correttezza** degli esponenti aziendali, che possono venir meno al verificarsi di situazioni pregiudizievoli tra cui, a titolo esemplificativo, le condanne non definitive, l'irrogazione di sanzioni amministrative, i provvedimenti disciplinari quali la radiazione o la sospensione da albi professionali, indagini e procedimenti penali in corso.

L'art. 5 si sofferma sulla **valutazione della correttezza,** che va condotta avendo riguardo ai principi di sana e prudente gestione, nonché alla salvaguardia della reputazione della banca e della fiducia del pubblico, in quanto il verificarsi della situazione pregiudizievole di cui all'art. 4 non comporta automaticamente l'inidoneità dell'esponente aziendale. Tale valutazione ha infatti un margine di discrezionalità ed è effettuata sulla base di una serie di parametri quali ad esempio l'oggettiva gravità dei fatti commessi, la frequenza dei comportamenti, l'importo della sanzione irrogata.

L'art. 6 riguarda la **sospensione degli incarichi**, che invece è automatica in caso di condanna a pena detentiva o misura cautelare personale ed è dichiarata senza indugio dall'organo competente e resa nota all'Autorità di vigilanza (BCE o Banca d'Italia per le banche meno significative).

Da ultimo, l'art. 7 individua i **requisiti di professionalità** facendo una chiara distinzione fra esponenti con incarichi esecutivi ed esponenti privi di tali incarichi. I primi verranno scelti tra persone che abbiano esercitato per almeno tre anni attività di amministrazione, direzione e controllo nel settore, oppure presso società quotate con dimensioni assimilabili a quelle della banca presso la quale l'incarico deve essere assunto. Per gli esponenti con incarichi non esecutivi sarà sufficiente una pregressa attività professionale meno

qualificata ([94]). Alla luce di queste disposizioni regolamentari si può affermare che nel settore bancario la previsione così puntuale di requisiti di onorabilità/professionalità pur non essendo un'autorizzazione esplicita al trattamento dei dati giudiziari, suggerisce un'autorizzazione indiretta al trattamento degli stessi al fine di verificare il possesso e la conservazione dei requisiti in capo ai soggetti destinatari del provvedimento.

Per quanto riguarda il **settore assicurativo** la norma primaria di riferimento sui requisiti di onorabilità, professionalità e indipendenza degli esponenti aziendali e dei soggetti che svolgono funzioni fondamentali è contenuta nell'art. 76 del Codice delle assicurazioni private (d.lgs. 7/9/2005 n. 209) da ultimo modificato dal d.lgs. 14/7/2020 n. 84.

Il decreto legislativo fornisce esecuzione all'art. 7 della legge 4/10/2019 n. 117 (legge di delegazione europea 2018) che recepisce la direttiva 828/2017/UE (*Shareholders' Rights Directive 2*) apportando modifiche alla disciplina di governo societario delle società assicuratrici, in particolare per quanto riguarda i requisiti e i criteri di idoneità degli esponenti aziendali, dei soggetti che svolgono funzioni fondamentali e dei partecipanti al capitale ([95]).

Sono quattro le principali innovazioni della norma entrata in vigore il 14 agosto 2020, per quanto qui rileva: **la prima** è la previsione di un generale requisito di idoneità all'incarico da parte degli esponenti aziendali di rilievo delle imprese di assicurazione; **la seconda** associa ai consueti requisiti di professionalità, onorabilità e indipendenza, anche quelli di competenza e correttezza; **la terza** attribuisce all'IVASS (Istituto per la Vigilanza sulle Assicurazioni) i poteri idonei di intervento nei confronti dei soggetti apicali che non soddisfano i requisiti e i criteri richiesti, compresa la possibilità di

([94]) F. CIVALE, *Requisiti e criteri di idoneità degli esponenti aziendali delle banche: prime riflessioni in margine al Decreto del MEF*, in www.dirittobancario.it, 21/12/2020.
([95]) P. CECCHINATO, *In G.U. il D.lgs. n. 84/2020 che dà compiuta attuazione alla SHRD2*, in *Quotidiano giuridico*, Milano, UTET, 31/7/2020.

dichiarare automaticamente la decadenza dei soggetti apicali in caso di carenza di detti requisiti, nonché di rimuoverli prontamente dall'incarico in caso di condotta ritenuta idonea a recare pregiudizio alla sana e prudente gestione aziendale; **la quarta** è il rinvio al regolamento adottato dal Ministro dello sviluppo economico, sentito l'IVASS, per l'individuazione dei requisiti sopra riepilogati, nonché delle cause che comportano la sospensione temporanea della carica e la sua durata. Viene altresì indicato che il decreto sarà adottato entro 180 giorni dalla entrata in vigore del decreto legislativo avvenuta il 14/8/2020. Al momento il decreto del Ministro dello sviluppo economico non è stato ancora pubblicato. Anche qui, come sopra affermato per il settore bancario, siamo in presenza di una previsione, che, ribadendo i requisiti di onorabilità/professionalità lascia intendere un'autorizzazione indiretta al trattamento dei dati giudiziari al fine di verificare che tali requisiti vengano posseduti e conservati.

In conclusione, si può sostenere che le imprese private di assicurazione, al pari di quelle bancarie siano autorizzate (anzi, obbligate) dalla legge e dal regolamento ministeriale al trattamento dei dati giudiziari (limitatamente a quelli espressamente richiamati dalle disposizioni normative sopra ricordate) dei soggetti che svolgono funzioni fondamentali e che partecipano al capitale della società.

4. Il trattamento dei dati giudiziari del lavoratore nella giurisprudenza nazionale antecedente al Regolamento UE 679/2016 e al d.lgs. n. 101/ 2018

Si ritiene utile sottolineare ora su un tema molto delicato come il confine tra il diritto alla riservatezza del lavoratore e l'interesse del datore di lavoro ad acquisire più informazioni possibili per valutare la competenza e l'affidabilità del candidato da assumere, riguardanti anche l'esistenza di procedimenti penali definiti o in corso. Bisogna chiedersi se il datore di lavoro al momento dell'assunzione può richiedere e trattare liberamente queste informazioni.

È bene però premettere ed evidenziare la differenza tra il "certificato del casellario giudiziale" e il "certificato dei carichi pendenti". Il testo unico in materia di casellario giudiziale approvato con il D.p.r. 14/11/2002 n. 313 integrato dal d.lgs. 2/10/2018 n. 122 (c.d. riforma Orlando) ([96]) distingue i due documenti separando la disciplina dei relativi certificati e della procedura di richiesta.

Per quanto riguarda il certificato del casellario giudiziale si tratta dell'iscrizione di "provvedimenti giudiziari penali di condanna definitivi", quindi reati commessi ed accertati giudizialmente; per quanto riguarda il certificato dei carichi pendenti si tratta dei procedimenti penali in corso a carico di un determinato soggetto e gli eventuali relativi giudizi di impugnazione rilasciato dalla Procura della Repubblica presso il Tribunale che ha giurisdizione sul luogo di residenza dell'interessato ([97]). Va ricordato che in passato, il comma 2 dell'art. 607 c.p.p., oggi abrogato, abilitava il

([96]) Per un esame più puntuale della riforma Orlando sul casellario giudiziale vedi M. F. CORTESI, *Prosegue il cammino della "riforma Orlando" anche in materia di casellario giudiziale*, in *Quotidiano giuridico*, Milano, UTET, 31/10/2018
([97]) La definizione è tratta dal sito del Ministero della Giustizia: www.giustizia.it

datore di lavoro a richiedere direttamente il certificato penale in sede di assunzione, pur subordinando la richiesta all'indicazione di un legittimo interesse ([98]).

Oggi la situazione è cambiata, e ferme restando le eccezioni che sono state riepilogate nei paragrafi precedenti (assunzioni presso la Pubblica Amministrazione, lavoro a contatto con i minori, settore bancario e assicurativo), il datore di lavoro non può fare direttamente richiesta del certificato del casellario giudiziale e dei carichi pendenti, in quanto, trattandosi di dati a carattere strettamente personale, possono essere acquisiti solamente dal diretto interessato.

Sulla base di un orientamento che si è pronunciato su fattispecie antecedenti all'entrata in vigore del d.lgs. 101 del 2018 della giurisprudenza della Corte di Cassazione, da ultimo con la sentenza della Sez. lav. 17/7/2018 n. 19012, la richiesta del certificato penale ai fini dell'assunzione integra un limite rispetto alla previsione di cui all'art. 8 dello Statuto dei lavoratori, che si giustifica con la rilevanza, ai fini della valutazione dell'attitudine professionale del lavoratore, della conoscenza dell'esistenza di condanne penali passate in giudicato. Ma tale limite, prosegue la stessa sentenza, in assenza di una previsione del Contratto Collettivo Nazionale di Lavoro, non può essere dilatato in via interpretativa fino a ricomprendere le informazioni relative a procedimenti penali in corso (carichi pendenti) in considerazione del principio costituzionale della presunzione di innocenza sancito all'art. 27.

La sentenza citata tratta il caso di una dipendente di Poste Italiane che non veniva assunta in servizio essendo risultato dalla certificazione prodotta in fase di assunzione al datore di lavoro un carico pendente. La lavoratrice chiedeva al Tribunale, di condannare la società ad immetterla in servizio. I Giudici, sia in primo che in secondo grado, accoglievano la domanda

[98] M. RUSSO, *Richiesta del certificato penale e del certificato carichi pendenti ai fini della assunzione*, in www.ilgiuslavorista.it, 2/7/2019.

sottolineando che il Contratto Collettivo Nazionale di Lavoro prevedeva la presentazione del certificato penale di data non anteriore a tre mesi, e non anche quello dei carichi pendenti. Poste Italiane ricorre in Cassazione sostenendo che l'espressione "certificato penale" debba essere intesa in senso ampio, comprensivo anche dei carichi pendenti.

La Cassazione chiarisce che l'art. 8 dello Statuto dei lavoratori vieta al datore di lavoro, sia in fase di assunzione che nel corso del rapporto di lavoro di effettuare indagini su fatti non rilevanti rispetto alla valutazione dell'attitudine professionale del lavoratore. Tale valutazione si fonda sulla conoscenza delle informazioni relative all'esistenza di condanne penali passate in giudicato, e non sui procedimenti penali in corso in virtù del principio costituzionale della presunzione d'innocenza dell'art. 27. In conclusione, la Corte rigetta il ricorso di Poste Italiane ([99]).

Si può affermare quindi che il datore di lavoro, potrà soltanto limitarsi, se previsto dalla contrattazione collettiva, a chiedere l'esibizione del certificato del casellario giudiziale, considerato che, in base all'art. 8 dello Statuto dei lavoratori e all'art. 27 della Costituzione, per valutare l'attitudine professionale del lavoratore rilevano soltanto le condanne penali passate in giudicato. Ciò potrà chiaramente avvenire solo quando interverrà l'apposita autorizzazione del Ministero della Giustizia che dovesse confermare le indicazioni sul "futuro" trattamento dei dati giudiziari sulla base di una previsione del contratto collettivo. Se dalla contrattazione collettiva di lavoro non risulta alcuna disposizione in tal senso, la richiesta del certificato del casellario giudiziale potrà essere lecita e giustificata solo con riferimento alla delicatezza delle mansioni che il lavoratore andrà a svolgere. Ovviamente, le indicazioni della giurisprudenza non possono essere considerate risolutive in

[99] Cass. sez. lav., sent. 17/7/2018 n. 19012 in www.dirittoegiustizia.it, 18/7/2018.

mancanza del predetto decreto ministeriale o di specifiche autorizzazioni legali.

Peraltro, la sentenza della Cassazione del 2018 ha fatto molto discutere ed è anche in contrasto con le statuizioni di una recente ordinanza della Corte di Cassazione, la n. 17167 del 2020, che ha stabilito i seguenti principi di diritto:

a) "il principio di non colpevolezza fino alla condanna definitiva, di cui all'art. 27 Cost. comma 2, concerne le garanzie relative all'attuazione della pretesa punitiva dello Stato, e **non può quindi applicarsi, in via analogica o estensiva, ai rapporti tra privati**";

b) "La società ha infatti esercitato il potere discrezionale...di **non procedere all'assunzione** di personale allorquando l'assunzione stessa si configuri come **incompatibile con le esigenze di affidabilità e piena funzionalità** dell'impresa privata, come avviene nel caso in cui l'attività dispiegata postuli una intensità della fiducia rapportata all'oggetto delle mansioni ed al grado di affidamento che queste richiedono".

Si può ritenere quindi che da un punto di vista strettamente giuslavoristico ci siano argomentazioni per ritenere consentito al datore di lavoro, anche in assenza di una espressa autorizzazione del contratto collettivo di lavoro, l'acquisizione di dati giudiziari ("provvisori" o "definitivi") del candidato qualora:

a) siano rilevanti per la valutazione della sua attitudine professionale (cfr. art. 8 della legge 300 del 1970);

b) siano coerenti con l'oggetto del contratto di lavoro (mansioni);

c) il grado di affidabilità e fiducia della posizione lavorativa di destinazione lo richieda.

Va detto però, in conclusione, che la questione non può essere affrontata esclusivamente con l'esame dei tradizionali concetti giuslavoristici, ma va confrontata necessariamente con la normativa sulla privacy.

È bene specificare, che per quanto attiene alla liceità del trattamento dei dati giudiziari dei dipendenti si è espressa anche la Autorità Garante per la protezione dei dati personali con il provvedimento n. 314 del 22/5/2018 ([100]) che ha ritenuto non accoglibile la richiesta avanzata da una società di fornitura di servizi informatici che si era rivolta al Garante per ottenere l'autorizzazione a trattare i dati giudiziari dei propri dipendenti che svolgevano mansioni riconducibili alle attività proprie dell'amministratore di sistema. La motivazione principale che ha portato alla decisione del Garante è che il datore di lavoro può richiedere il certificato del casellario giudiziale solo in presenza di un'idonea base giuridica, sia essa legislativa o regolamentare, valutando se risultano applicabili al caso concreto disposizioni dell'ordinamento che prevedano il trattamento di dati giudiziari dei dipendenti in relazione alle attività svolte dalla società, analogamente a quanto espressamente previsto dal legislatore per determinate attività, come ad esempio le attività professionali o volontarie a contatto con minori e le attività di amministrazione, direzione e controllo presso le imprese di assicurazione.

([100]) Garante per la Protezione dei Dati Personali, Provvedimento n. 314 del 22/6/2018, Doc. web n. 9005845.

CAPITOLO III

Il trattamento dei dati sanitari nel rapporto di lavoro

SOMMARIO: 1. L'evoluzione normativa del dato sanitario fino al Regolamento UE 679/2016. - 2. La nozione e il trattamento dei dati sanitari nel Regolamento UE 679/2016 e nel codice della privacy. - 3. Il trattamento dei dati sanitari del lavoratore: tre casi tra tutela della salute e protezione della riservatezza. – 4. La disciplina emergenziale sul trattamento dei dati sanitari. – 4.1. Il Protocollo tra il Governo e le parti sociali del 14 marzo 2020. - 4.2. Le indicazioni dei Garanti privacy europei sul trattamento dei dati sanitari in emergenza. - 5. Trattamento dei dati sanitari, test diagnostici e vaccino anti COVID – 19: questioni e orientamenti del Garante della privacy italiano.

1. L'evoluzione normativa del dato sanitario fino al Regolamento UE 679/2016

Già nel Codice civile, all'art 2087, pur non esistendo ancora la nozione di dato sanitario né i principi in materia di trattamento nel rapporto di lavoro, viene tenuta in particolare considerazione la tutela delle condizioni di lavoro e l'imprenditore "è tenuto ad adottare nell'esercizio dell'impresa le misure che, secondo la particolarità del lavoro, l'esperienza e la tecnica, sono necessarie a tutelare l'integrità fisica e la personalità morale del prestatore di lavoro". Tale norma vuole garantire l'integrità fisica e la personalità morale del lavoratore, ricomprendendo nella sua disposizione qualsiasi atteggiamento pregiudizievole per la persona che lavora in tutte le sue dimensioni. Si può senz'altro affermare che l'art. 2087 si inserisce nel contesto delle disposizioni che presiedono alla tutela della salute del lavoratore ([101]), e sembra anticipare uno dei principi sul trattamento dei dati sanitari che riguarderà, molti anni più tardi, la possibilità di trattamento dei dati sanitari per la valutazione della capacità lavorativa dei dipendenti.

Con lo Statuto dei lavoratori del 1970 e in particolare all'art. 5, rubricato "Accertamenti sanitari" si dispone che: "Sono vietati accertamenti da parte del datore di lavoro sulla idoneità e sulla infermità per malattia o infortunio del lavoratore dipendente. Il controllo delle assenze per infermità può essere effettuato soltanto attraverso i servizi ispettivi degli istituti previdenziali competenti, i quali sono tenuti a compierlo quando il datore di lavoro lo richieda. Il datore di lavoro ha la facoltà di far controllare l'idoneità

([101]) P. PASCUCCI, A. DELOGU, *Salute e sicurezza nei luoghi di lavoro, in Diritto e processo del lavoro e della previdenza sociale*, *Tomo secondo*, G. SANTORO-PASSARELLI, (a cura di), Milano, UTET, 2020.

fisica del lavoratore da parte di enti pubblici ed istituti specializzati di diritto pubblico".

Si nota come attraverso tale norma la libertà e la dignità del lavoratore vengono ulteriormente salvaguardate attraverso una particolare limitazione dei poteri del datore di lavoro. Si tratta in questo caso del potere del datore di lavoro di sottoporre a verifica sanitaria le certificazioni di malattia e infortunio dei lavoratori dipendenti. Per la prima volta, si fa divieto al datore di lavoro di utilizzare per gli accertamenti sanitari, medici di propria fiducia, come i c.d. medici di fabbrica, imponendogli di ricorrere a medici appartenenti a organismi pubblici, che successivamente saranno identificati nelle ASL e nell' INPS ([102]). Il legislatore pertanto rende imparziale il meccanismo dei controlli fiscali relativi alle malattie e agli infortuni dei lavoratori, e consente al datore di lavoro di trattare il "dato sanitario" della malattia e dell'infortunio con tutte le possibili tutele in quel momento storico. Alle istituzioni pubbliche competenti il datore di lavoro può rivolgersi anche per far controllare l'idoneità fisica del lavoratore, ossia l'esistenza non solo di un'alterazione temporanea dello stato di salute (come nel caso della malattia o dell'infortunio), ma anche di una situazione di sopravvenuta incapacità allo svolgimento delle mansioni ([103]).

Va ricordato che la norma dello Statuto, oltre a garantire che gli accertamenti vengano condotti da enti pubblici e non da medici di fiducia del datore di lavoro, vuole salvaguardare il rispetto della dignità e della riservatezza del lavoratore sottoposto a visita. Allo stesso tempo vuole eliminare la discriminazione che si verrebbe a creare qualora il datore di lavoro ottenesse informazioni sullo stato di salute dei lavoratori non strettamente connesse con le mansioni dedotte in contratto. Inoltre, non è da

([102]) R. DEL PUNTA, F. SCARPELLI, *Art. 5 dello Statuto dei lavoratori in Codice commentato del lavoro, Ed. I*, Milano, IPSOA, 2019.
([103]) G. PROIA, *Manuale di diritto del lavoro, Ed. III*, Padova, CEDAM, 2020.

escludere che la previsione dell'art. 5 possa integrarsi con i divieti dell'art. 8 dello Statuto dei lavoratori, qualora dalla indagine consentita sulla idoneità fisica del lavoratore si giunga, in qualsiasi modo, ad ottenere informazioni su fatti non rilevanti ai fini della prestazione ([104]).

Nel tempo, con l'introduzione delle leggi in materia di riservatezza e protezione dei dati personali, anche i dati relativi alla salute di una persona fisica sono stati oggetto di indagine e di maggior tutela in quanto dati strettamente personali. In ambito comunitario il Comitato dei Ministri del Consiglio d'Europa era intervenuto con la Raccomandazione n. 81/1981([105]) con la quale furono individuati "i criteri di gestione delle banche di dati sanitari automatizzati, fornendo un serie di importanti direttive per l'utilizzo di tali banche dati, nei limiti in cui la coeva Convenzione di Strasburgo ne consentiva la creazione". La stessa Raccomandazione al punto 5.4 disponeva che "senza il consenso espresso e cosciente della persona interessata, l'esistenza e il contenuto di un dossier sanitario che la riguardi non può essere comunicato a persone o organismi fuori dal campo delle cure mediche, della sanità pubblica o della ricerca medica, a meno che una tale comunicazione non sia permessa dalle regole del segreto professionale dei medici." Si comprende come tale affermazione dimostri l'importanza di garantire e tutelare dati sanitari che consentono l'individuazione della persona alla quale sono riferiti o riferibili.

Negli anni immediatamente successivi inizierà ad elaborarsi la disciplina dei c.d. dati sensibili, di cui una importante categoria è costituita dai dati sanitari, ossia, come si legge nell'art. 17 della proposta di Direttiva 24/9/1990 della Commissione delle Comunità Europee, quelle "informazioni

([104]) C. LAZZARI, *Le visite di pre-assunzione fra divieto di analogia, potenzialità discriminatorie e tutela della riservatezza*, in *Giurisprudenza Italiana*, 4/1999.
([105]) Direttiva 81/1981 del Comitato dei Ministri del Consiglio d'Europa relativa alla regolamentazione applicabile alle banche di dati sanitari automatizzate, in www.privacy.it, 23/1/1981.

riguardanti la salute della persona interessata (comprese quelle sullo stato fisico e mentale passato, presente o futuro della persona interessata e le informazioni sull'abuso di droga e alcol)". Può considerarsi questa la prima nozione di dato sanitario rinvenuta in una comunicazione istituzionale.

Ci si trova nel periodo in cui le banche dati stavano nascendo e sviluppandosi, e permettendo la elaborazione di queste particolari informazioni, da una parte devono trattare grandi quantità di dati per consentire di fornire al meglio prevenzione, cure e servizi medici e dall'altra provano a rispettare dignità e privacy della persona interessata. Tutte le proposte di legge che nei primi anni '90 si susseguirono in tema di trattamento di dati sensibili e in particolare dei dati sanitari tendevano a realizzare attraverso sottili equilibri una tutela della salute e non un potere sulla salute ([106]).

Nell'attesa dell'approvazione di una prima legge in Italia in materia che avverrà nel 1996 si registrava una situazione di assoluta carenza di regole precise per gli operatori del settore, rimanendo i dati sanitari affidati unicamente alla correttezza di chi gestiva tali informazioni, e in questo caso alla deontologia professionale della categoria medica.

Con la legge 31/12/1996 n. 675 viene approvata la prima disposizione nazionale in materia di riservatezza all'interno della quale si trova l'art. 23 rubricato come "dati inerenti alla salute" che stabilisce tre principi cardine. Il primo è che solo gli esercenti le professioni sanitarie e gli organismi sanitari possono trattare i dati inerenti alla salute. Per chiunque altro il trattamento può avvenire solo previa autorizzazione del Garante della Privacy. Il secondo principio è che i dati inerenti alla salute possono essere resi noti all'interessato solo per il tramite di un medico designato dall'interessato stesso. Il terzo è che la diffusione dei dati idonei a rivelare lo stato di salute è vietata salvo nel

([106]) G. CIACCI*, Problemi e iniziative in tema di tutela dei dati personali con particolare riguardo ai dati sanitari*, in *Politica del diritto*, Bologna, Il Mulino, 1991.

caso in cui sia necessaria per finalità di prevenzione, accertamento o repressione dei reati.

Con il d.lgs. 30/6/2003 n. 196 (Codice privacy) venivano poi apportate delle modifiche alla precedente legge del ’96 assegnando per la prima volta un ruolo centrale alla materia relativa al consenso dell’interessato, ritenuto presupposto legittimante e condizione di liceità del trattamento dei dati sanitari, cosicché gli esercenti le professioni sanitarie e gli organismi sanitari pubblici avrebbero potuto trattare i dati personali idonei a rivelare lo stato di salute: a) con il consenso dell’interessato e anche senza l’autorizzazione del Garante, se il trattamento riguarda dai e operazioni indispensabili per perseguire una finalità di tutela della salute o dell’incolumità fisica dell’interessato; b) anche senza il consenso dell' interessato e previa autorizzazione del Garante se la finalità di cui alla lettera a) riguarda un terzo o la collettività.

Tale norma, come vedremo di seguito, verrà poi modificata e riformata dal regolamento UE 2016/679 e dal d.lgs. 101/2018 in materia di trattamento di dati sanitari.

2. La nozione e il trattamento dei dati sanitari nel Regolamento UE 679/2016 e nel Codice della privacy

La nozione e il trattamento dei dati sanitari sono ambedue disciplinati nel Regolamento UE 679/2016 cui è stata data attuazione in Italia dal d.lgs. n. 101/2018 che ha apportato alcune modifiche al Titolo V del d.lgs. 196/2003 (Codice della privacy) disciplinante il "Trattamento di dati personali in ambito sanitario."

Il GDPR offre all'art. 4 n. 15 una nozione di "dati relativi alla salute" da intendersi come: "i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute", e puntualizza al considerando 35 che "nei dati personali relativi alla salute dovrebbero rientrare tutti i dati riguardanti lo stato di salute dell'interessato che rivelino informazioni connesse allo stato di salute fisica o mentale passata, presente o futura dello stesso. Questi comprendono informazioni sulla persona fisica raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria o della relativa prestazione di cui la direttiva 2011/24/UE del Parlamento Europeo e del Consiglio; un numero, un simbolo o un elemento specifico attribuito a una persona fisica per identificarla in modo univoco a fini sanitari; le informazioni risultanti da esami e controlli effettuati su una parte del corpo o una sostanza organica, compresi i dati genetici e i campioni biologici; e qualsiasi informazione riguardante, ad esempio, una malattia, una disabilità, il rischio di malattie , l'anamnesi medica, i trattamenti chimico clinici o lo stato fisiologico o più medico dell' interessato, indipendentemente dalla fonte, quale, ad esempio, un medico o altro operatore sanitario, un ospedale, un dispositivo medico o un test diagnostico in vitro."

Si tratta evidentemente di una nozione particolarmente ampia di dato sanitario, in cui l'obiettivo è quello di consentire una copertura più estesa del Regolamento e quindi, di offrire una protezione maggiore ai singoli anche alla luce degli sviluppi legislativi in materia di assistenza sanitaria al di là dei confini di ciascuno Stato membro ([107]).

Indubbiamente, l'efficacia applicativa di tale nozione dipende in maniera significativa sia dal titolare del trattamento, competente a determinare le finalità e i mezzi del trattamento dei dati personali, sia dal responsabile del trattamento, competente a trattare i dati personali per conto del titolare stesso.

In merito al trattamento dei dati sanitari, poi, è lo stesso GDPR che all'art. 9 si sofferma con alcune disposizioni che si pongono in stretta connessione con i temi della salute ([108]).

La prima norma di riferimento contenuta nel primo comma è un generale divieto di trattamento dei dati relativi alla salute. Naturalmente, quello che in questa sede più interessa, sono le disposizioni che nei commi successivi ammettono, come eccezione, il trattamento di questi dati e per quali finalità.

Si tratta dell'art. 9 par. 2 lett. g), h) e i) ([109]) La **prima ipotesi** riguarda i motivi di interesse pubblico rilevante sulla base del diritto dell'Unione e degli Stati membri.

([107]) G. DI FEDERICO, S. NEGRI, *Unione Europea e salute*, Padova, CEDAM, 2020

([108]) R. TUCCILLO, *Art. 9 Regolamento UE n. 2016/679 – Trattamento di categorie particolari di dati personali – Par. 4.8 Tutela delle particolari categorie di dati e salute, op. cit.*

([109]) Art. 9 Reg. (UE) 27 aprile 2016, n. 679: "1. È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute alla vita sessuale o all'orientamento sessuale della persona. 2. Il paragrafo 1 non si applica se si verifica uno dei seguenti casi: […] g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità

La **seconda ipotesi** riguarda i casi in cui il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, per la valutazione della capacità lavorativa del dipendente, per la diagnosi, assistenza o terapia sanitaria o sociale ovvero per la gestione dei sistemi e servizi sanitari o sociali, sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità.

Il trattamento di tali dati deve essere eseguito sotto la responsabilità di un professionista soggetto al segreto professionale o da altra persona soggetta ad analogo obbligo di riservatezza. Conseguentemente, come chiarito dal Garante della privacy nel provvedimento n. 55 del 7/3/2019, ("Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario") lo stesso professionista sanitario, soggetto al segreto professionale, non dovrà chiedere il consenso del paziente per i trattamenti necessari alla prestazione sanitaria richiesta dall'interessato, indipendentemente dalla circostanza che operi in qualità di libero professionista, presso uno studio medico o all'interno di una struttura sanitaria pubblica o privata. Naturalmente siamo qui in presenza di trattamenti "necessari" al perseguimento delle specifiche "finalità di cura" previste dalla norma. Diversamente i trattamenti "non strettamente necessari" richiedono, anche se effettuati da professionisti della sanità, una distinta base giuridica da individuarsi o nel consenso dell'interessato o in un altro presupposto di liceità. Il Garante menziona, a titolo esemplificativo, i

perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare diritti fondamentali e gli interessi dell' interessato; h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte Salve le condizioni e le garanzie di cui al paragrafo 3; i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, nei quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell' interessato, in particolare il segreto professionale".

trattamenti connessi all'utilizzo di App mediche, quelli preordinati alla fidelizzazione della clientela o effettuati dalle farmacie attraverso programmi di accumulo punti.

La **terza ipotesi** riguarda fattispecie eterogenee quali i trattamenti giustificati dalla protezione di gravi minacce per la salute a carattere transfrontaliero, dalla garanzia di elevati parametri di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dispositivi medici.

Il legislatore italiano, nel Codice della Privacy opportunamente aggiornato dal d.lgs. 101/2018 recepisce le disposizioni del GDPR in tema di trattamento all'art. 75 nel quale si dispone che: "il trattamento dei dati personali effettuato per finalità di tutela della salute e incolumità fisica dell' interessato o di terzi o della collettività deve essere effettuato ai sensi dell'articolo 9 par. 2 lettere h) ed i), e 3 del Regolamento, dell'articolo 2-septies del presente codice, nonché nel rispetto delle specifiche disposizioni di settore".

Si ribadisce, pertanto, che il trattamento dei dati sanitari trova la sua base giuridica nel carattere necessario del trattamento per finalità di medicina preventiva o di medicina sul lavoro, o perché strumentale al perseguimento di interessi pubblici nell'ambito della sanità pubblica ([110]).

Va detto infine che il legislatore italiano ha previsto con l'art. 2-*septies* ("Misure di garanzia per il trattamento di dati genetici, biometrici e relativi alla salute") del Codice della privacy novellato, misure di garanzia fissate dal Garante e riviste con cadenza biennale. Conseguentemente, il Garante adotta le misure, sentito il Consiglio superiore di sanità e tenendo conto delle linee guida, delle raccomandazioni e delle buone prassi del Garante europeo, in particolare con riferimento alle cautele relative alle modalità per la

([110]) M. MARTORANA, A. TESORO, *Le informazioni da fornire all'interessato e le modalità di raccolta del consenso ai sensi del d.lgs. 101/2018* in M. MARTORANA, (a cura di) *GDPR e decreto legislativo 101/2018*, Padova, CEDAM, 2019.

comunicazione diretta all'interessato delle diagnosi e dei dati relativi alla propria salute, nonché della evoluzione tecnologica e scientifica del settore a cui tali misure sono rivolte e l'interesse alla libera circolazione dei dati nel territorio Europeo. Inoltre, sempre l'Autorità di controllo dovrà anche promuovere le regole deontologiche per il trattamento dei dati relativi alla salute ([111]).

([111]) Per un esame dettagliato delle misure di adeguamento al Regolamento 679/2016 si veda Servizio Studi Camera dei deputati, *L'adeguamento della disciplina sulla protezione dei dati personali al Regolamento (UE) 2016/679*, Dossier n. 18, Atti del governo n. 22, 21/5/2018.

3. Il trattamento dei dati sanitari dei lavoratori: tre casi tra tutela della salute e protezione della riservatezza

La normativa sui dati sanitari così come sopra riepilogata, va analizzata ora in relazione alla disciplina lavoristica con particolare riferimento al bilanciamento tra la tutela della salute nell'ambiente di lavoro e la protezione dei dati di carattere personale. Ovviamente potrebbero essere molteplici le fattispecie da valutare in quest'ottica, ma in questa sede ci si soffermerà solo su tre casi emblematici.

La **prima fattispecie** riguarda l'interpello del Ministero del lavoro n. 4/2019 ([112]) che offre una riflessione sugli obblighi del datore di lavoro in merito alla sorveglianza sanitaria dei lavoratori alla luce della più recente normativa in tema di privacy.

È stata la Federazione Nazionale dei Medici Chirurghi e Odontoiatri a porre il quesito sulla possibilità di inserire in un *data base* aziendale, amministrato dal datore di lavoro o da un dipendente appositamente individuato allo scopo, i dati sanitari completi dei lavoratori anziché il solo giudizio di idoneità e le relative prescrizioni.

Il Ministero anzitutto conferma la possibilità di utilizzo di sistemi informatici gestiti dal datore di lavoro per memorizzare qualunque tipo di documento previsto dal d.lgs. 81/2008 ([113]), evidenziando, peraltro, la necessità di adottare "soluzioni concordate tra datore di lavoro e medico competente che, nel rispetto del segreto professionale e della tutela della privacy, garantiscano l'accessibilità ai suddetti dati soltanto al medico

([112]) Interpello n. 4 del 28/5/2019 ai sensi dell'art. 12 del d.lgs. n. 81/2008 e successive modificazioni-Tenuta della documentazione sanitaria su supporto informatico, in www.lavoro.gov.it.
([113]) Decreto legislativo 9/4/2008 n. 81, Attuazione dell'art. 1 della legge 3 agosto 2007 n. 123, in materia di tutela della salute e della sicurezza nei luoghi di lavoro, in *Gazzetta Ufficiale* n. 101 del 30/4/2008.

competente e non permettano né al datore di lavoro né all' amministratore di sistema di potervi accedere."

È necessario ricordare che il decreto legislativo 81/2008 impone al datore di lavoro, per il tramite del medico competente, di effettuare: a) accertamenti preventivi volti a constatare l'assenza di controindicazioni al lavoro cui il lavoratore è destinato; b) accertamenti periodici per controllare lo stato di salute dei lavoratori ed esprimere il giudizio di idoneità alla mansione specifica.

I dati che ne conseguono, comprendenti gli esami clinici, biologici e le indagini diagnostiche, confluiscono nella cartella sanitaria e di rischio del lavoratore che contiene la sua storia clinica, familiare e lavorativa. Si tratta, in sostanza, di dati particolari ai sensi dell'art. 9 del GDPR che, come tali non possono essere trattati se non in situazioni specificatamente individuate, tra le quali rientra, come sopra ricordato, il caso in cui "il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria sociale ovvero gestione di sistemi e servizi sanitari o sociali" (art. 9 comma 2 lett. h) del GDPR). Tali dati dovranno poi essere trattati da un professionista soggetto al segreto professionale (art. 9 comma 3 del GDPR).

La normativa sulla tutela della salute e della sicurezza nei luoghi di lavoro vuole assicurare che l'accesso ai dati sanitari dei lavoratori sia consentito unicamente al medico competente ed a persone appositamente autorizzate, e prevede a riguardo che: da una parte, il **datore di lavoro** possa essere informato unicamente circa il giudizio di idoneità, inidoneità o idoneità con prescrizioni o limitazioni alla mansione specifica ricoperta dal lavoratore, ma non possa conoscere la diagnosi svolta dal medico; dall'altra, il **medico competente** istituisce, aggiorna e custodisce sotto la propria responsabilità, una cartella sanitaria e di rischio per ogni lavoratore sottoposto a sorveglianza

sanitaria che conserverà con salvaguardia del segreto professionale presso il luogo di custodia concordato con il datore di lavoro al momento della sua nomina. Tutta la documentazione, sia su supporto cartaceo che informatico deve essere custodita nel rispetto della normativa sulla protezione dei dati personali.

In conclusione, la risposta del Ministero del lavoro al quesito della Federazione dei medici, considera possibile memorizzare la cartella sanitaria in un *data base* aziendale sottolineando però la necessità di assicurare l'accessibilità alla cartella solamente al medico competente, che oltre ad avere un apposito obbligo di segretezza, deve garantire che né il datore di lavoro, né qualsiasi altro amministratore di sistema possano in qualsiasi modo venire a conoscenza dei dati in essa contenuti ([114]).

Sul tema della tutela della privacy e del trattamento dei dati sanitari in ambito lavorativo assume poi rilievo una **seconda fattispecie** concreta, sulla quale si sono pronunciate le Sezioni Unite della Cassazione con sentenza n. 30981 del 27/12/2017 ([115]) intervenendo a risolvere un contrasto sul trattamento dei dati concernenti la salute, che possono essere trattati soltanto mediante tecniche di cifratura o criptatura che rendano non identificabile l'interessato.

La fattispecie su cui si è confrontata la Cassazione ha riguardato la causale del bonifico richiesto in favore di un beneficiario dell'indennizzo previsto dalla legge 25/2/1992 n. 210 per coloro che abbiano riportato, a causa di vaccinazioni obbligatorie (anche per motivi di lavoro o per incarico del loro ufficio) una menomazione permanente dell'integrità psicofisica, o a chi risulti contagiato da infezioni HIV, o che presenti danni irreversibili da epatite post-trasfusionale. L'indennizzo consiste in un assegno, reversibile per 15

([114]) L. MONTEMEZZO, *La sorveglianza sanitaria dei lavoratori: fra tutela della salute e protezione della privacy,* in www.buttiandpartners.com, 23/10/2019.
([115]) Cass. SU 27/12/2017 n. 3098, in *Foro italiano*, I, 2147, 2018.

anni, ovvero in un assegno *una tantum* erogato dallo Stato, in favore della vittima o dei suoi eredi.

Secondo un primo indirizzo della Corte, il riferimento all'indennità di cui alla legge 210/92 contiene un dato personale che va trattato con le cautele indicate dalla normativa sulla privacy, e quindi va trattato con tecniche di cifratura o mediante codici identificativi che li rendano temporaneamente inintellegibili a chi è autorizzato ad accedervi. Differentemente, in altra pronuncia della stessa Corte si è negato alla causale di bonifico la natura di dato particolare, avendo i giudici rilevato che l'informazione dell'elargizione dell'assegno non fosse sufficiente a dimostrare lo stato di salute del beneficiario. Inoltre, anche qualora la dizione dell'assegno fosse inquadrabile tra i dati particolari, la sua comunicazione sarebbe stata comunque lecita in quanto autorizzata da specifiche disposizioni di legge.

Le Sezioni Unite risolvono il contrasto ritenendo che lo Stato e la banca siano tenuti (in qualità di titolari di trattamento di dati personali nel procedimento di riconoscimento, erogazione e accredito dell'indennità di cui alla legge n. 210/92) a occultare mediante tecniche di cifratura o criptatura il riferimento a tale legge in quanto idoneo a rivelare lo stato di salute del beneficiario dell'indennità.

La Corte chiarisce come la natura "super sensibile" dei dati sanitari connessi al riconoscimento dell'indennità in questione è riconosciuta dalla stessa legge n. 210/1992, che nell'art. 3 prevede che l'istruzione della domanda avvenga in modo da garantire "il diritto alla riservatezza anche mediante opportune modalità organizzative" e la garanzia di riservatezza viene estesa a "chiunque nell'esercizio delle proprie funzioni venga a conoscenza" di persone danneggiate da complicanze di tipo irreversibile a causa di vaccinazioni obbligatorie, trasfusioni, e somministrazioni di emoderivati.

Va imposto pertanto l'obbligo di cifratura o criptatura, non soltanto limitato ai dati contenuti in elenchi, registri o banche dati, tenute con l'ausilio di strumenti elettronici, ma va esteso a tutte le modalità di raccolta dei dati anche meramente cartacee.

La sentenza delle Sezioni Unite, anche se interviene sulla disciplina antecedente al GDPR, afferma principi che devono ritenersi vigenti anche nel nuovo assetto normativo, che si caratterizza per un rafforzamento della protezione dei dati sanitari. Basti ricordare che l'art. 32 del GDPR prescrive la necessità di mettere in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio, tra le quali, la pseudonimizzazione e la cifratura dei dati personali ([116]).

Ancora sul trattamento dei dati sanitari del lavoratore e sulla tutela della privacy assume rilievo una **terza fattispecie** su cui si è espressa la Corte di Cassazione con l'ordinanza 16560/2020 ([117]), dichiarando inammissibile il ricorso di un infermiere contro la decisione del Garante della privacy relativa a un caso di comunicazione dei dati in materia di sorveglianza sanitaria.

Il caso si riferisce ad una caposala di ospedale, che con nota interna alla dirigente dell'ufficio infermieristico, alla referente per le aree esterne e alla coordinatrice del dipartimento di psichiatria, comunicava l'opportunità della sottoposizione a visita straordinaria del proprio dipendente, ai sensi del d.lgs. 81/2008, per "problemi di iperglicemia" e per la correlata periodica sottoposizione "a trattamenti di plasmaferesi in regime di *day-hospital.*"

L'infermiere si rivolgeva al Garante privacy e lamentava una violazione grave dei suoi diritti, nel caso di specie il suo diritto alla privacy, relativamente alla sopracitata comunicazione dei propri dati sanitari ad opera della caposala. Il Garante si esprimeva sulla fattispecie affermando che non

([116]) G. GRASSO, *Tutela della privacy e trattamento dei dati sensibili* in *Il libro dell'anno del diritto*, Roma, Istituto Enciclopedia Italiana, 2019.
([117]) Cass. Sez. I civ. Ordinanza 16560/2020, in www.dirittoegiustizia.it, 3/8/2020.

esisteva nel caso in esame una concreta violazione della privacy, avendo inteso la nota della caposala come una mera richiesta interna inoltrata ai superiori gerarchici. Inoltre, la sopra citata comunicazione rientrava nel novero dell'art. 5 dello Statuto dei lavoratori, che consente al datore di lavoro di far controllare l'idoneità fisica del lavoratore da parte di enti pubblici ed istituti specializzati di diritto pubblico. Il dipendente presenta ricorso contro la decisione del Garante al Tribunale di Roma, facendo notare come la comunicazione dei suoi dati sanitari andasse in violazione del principio di pertinenza e necessità, in quanto nella comunicazione venivano specificati la malattia dell'interessato e le terapie ivi connesse. Il Tribunale respinge il ricorso evidenziando due aspetti: il primo è che la segnalazione della caposala fosse "di carattere interno rivolta ai diretti superiori della coordinatrice" e che fosse motivata dall'esigenza superiore di tutela della salute del prestatore di lavoro e dei terzi utenti del servizio; il secondo è che la tutela della riservatezza si sarebbe affievolita in presenza di dati già divulgati dallo stesso interessato (ex art. 82 del Codice della privacy), considerando che la pubblica ostensione dei dati sanitari fosse una forma di consenso implicito al loro trattamento, in quanto lo stesso infermiere, autonomamente, aveva già reso partecipi alcuni dei propri colleghi della sua patologia.

L'interessato ricorre in Cassazione, la quale rigetta la domanda, conferma la ricostruzione in fatto e in diritto del Tribunale e dichiara inammissibile il ricorso evidenziando come la ricostruzione della modalità di gestione del dato secondo i canoni di correttezza, pertinenza e non eccedenza, integri una questione di fatto che esorbita dai confini del giudizio di legittimità della Corte.

Il caso in esame si riferisce ad una vicenda del 2010, precedente quindi rispetto al GDPR. Si è osservato che l'infermiere potrebbe oggi grazie alla tutela offertagli dal Regolamento europeo rivolgersi al *Data Protection Officer* (DPO), o Responsabile per la protezione dei dati personali, funzione

specialistica di presidio e di garanzia nonché obbligatoria nel comparto pubblico ([118]).

([118]) M. ALOVISIO, *Non viola la privacy la comunicazione dei dati sanitari del dipendente se è già resa nota dallo stesso*, in *Quotidiano Giuridico*, Milano, UTET, 15/9/2020.

4. La disciplina emergenziale sul trattamento dei dati sanitari

In data 31 gennaio 2020 il Consiglio dei ministri ha dichiarato lo stato di emergenza su tutto il territorio nazionale relativamente al rischio del potenziale proliferarsi di patologie derivanti da agenti virali relativi al Coronavirus[119]. Da questo momento in poi, tutte le disposizioni relative al trattamento dei dati personali, ivi inclusi, ovviamente, quelli sanitari, devono ritenersi adottate nel contesto di una situazione di emergenza, pur dovendo rispettare le garanzie previste dalla normativa in materia di protezione dei dati personali. Puntualmente, e non a caso, il Garante per la privacy con provvedimento n. 15 del 2 febbraio 2020 indica che alla scadenza del termine dello stato di emergenza, tutte le Amministrazioni coinvolte, adottino misure idonee a ricondurre i trattamenti effettuati nel contesto dell'emergenza nell'ambito delle ordinarie competenze ([120]).

Nella situazione di emergenza sanitaria dovuta alla pandemia da COVID-19 si sono verificate numerose ed evidenti implicazioni sul piano della riservatezza derivanti dal trattamento in maniera esponenziale dei dati sanitari dei lavoratori da parte dei datori di lavoro. Inoltre, l'aggravarsi della situazione di emergenza sanitaria e la necessità di dare continuità alle attività aziendali, laddove queste venivano consentite dalla normativa emergenziale, ha determinato una sorta di attenuazione al divieto generale di trattamento dei dati sanitari da parte dei titolari di azienda. Ma vediamo di seguito quali garanzie abbiano ritenuto di dover apportare a riguardo Governo e parti sociali.

([119]) Delibera del Consiglio dei ministri 31/1/2020, Dichiarazione dello stato di emergenza in conseguenza del rischio sanitario connesso all'insorgenza di patologie derivanti da agenti virali trasmissibili, in *Gazzetta Ufficiale* n. 26 dell'1/2/2020.
([120]) M. FESTA, *Coronavirus: il Garante privacy si esprime sulla richiesta di parere chiesto dalla protezione civile, in Quotidiano Giuridico*, Milano, UTET, 14/2/2020.

4.1 Il Protocollo tra il Governo e le parti sociali del 14 marzo 2020

Tale attenuazione si ritrova palesemente nel **Protocollo ([121])** di intesa sottoscritto il 14/3/2020, su invito del Governo, da Confindustria, Confapi, Rete Imprese per l'Italia, CGIL, CISL e UIL, poi integrato il 24 aprile successivo, aggiornato e rinnovato 6 aprile 2021.

Va detto che a tale Protocollo è sopravvenuto il d.p.c.m. 26/3/2020 (successivamente reiterato anche nel d.p.c.m. 3/12/2020) il cui art. 2 comma 6 ha imperativamente imposto il rispetto del contenuto del Protocollo pubblicato in Gazzetta Ufficiale come allegato del decreto. Conseguentemente il Protocollo ha perduto l'originaria forma negoziale, per fondersi con la natura autoritativa dell'atto amministrativo che lo ha recepito.

Va anzitutto evidenziato che in forza del Protocollo, l'alternativa in capo al datore di lavoro che non rispetta e che non fa rispettare le misure straordinarie, è quella di bloccare e sospendere la propria attività.

Riepilogando brevemente i **contenuti** del Protocollo, va detto che questo disciplina l'adozione di una molteplicità di misure di contrasto alla diffusione del virus COVID-19 negli ambienti di lavoro, aventi ad oggetto le modalità di ingresso in azienda di dipendenti e fornitori esterni, la sanificazione dei locali aziendali, le precauzioni logistiche e igieniche da osservare negli spazi aziendali comuni (quali mensa e spogliatoi) e in situazioni esposte al rischio di assembramento, quali ad esempio, *smart working,* ferie e permessi, turnazione, trasferte, ed infine, soprattutto, le modalità di attuazione della sorveglianza sanitaria in azienda e di gestione di una persona sintomatica.

([121]) Protocollo condiviso di regolamentazione delle misure per il contrasto e il contenimento della diffusione del virus COVID-19 negli ambienti di lavoro, del 14/3/2020, successivamente integrato il 24/4/2020, in allegato 12 al D.p.c.m 3/12/2020, in *Gazzetta Ufficiale*, n. 301, 3/12/2020, aggiornato e rinnovato il 6/4/2021 in www.salute.gov.it.

Le misure previste dal Protocollo sono alquanto delicate ed impattano fortemente sulla tutela dei diritti alla vita privata e alla protezione dei dati personali dei lavoratori interessati, ma allo stesso tempo chiamano il datore di lavoro a dare attuazione alle misure anti-contagio per delega della pubblica autorità. Basti dire, in sintesi, che il Protocollo: 1) riconosce al datore di lavoro la facoltà di sottoporre il personale aziendale al controllo della temperatura corporea prima dell'accesso al luogo di lavoro, con la conseguente interdizione dell'accesso nel caso in cui la temperatura rilevata sia superiore ai 37,5°, senza associarla all'identità dell'interessato; 2) indica alla persona presente in azienda che sviluppi sintomi di possibile contagio di dichiararlo immediatamente all'ufficio del personale, il quale ne dispone l'isolamento e provvede ad avvertire le autorità competenti; 3) stabilisce che l'ingesso in azienda di lavoratori già risultati positivi all'infezione dovrà essere preceduto da certificazione medica da cui risulti la avvenuta negativizzazione; 4) incarica il datore di lavoro di collaborare con le autorità sanitarie per tracciare gli eventuali contatti stretti di una persona presente in azienda risultata positiva al tampone COVID-19, cosi da permettere la applicazione delle necessarie misure di quarantena; 5) richiama il medico competente a segnalare all'azienda situazioni di particolare fragilità e patologie attuali o pregresse dei dipendenti ([122]).

Per quanto riguarda la **base giuridica** che consente alla normativa in questione di trattare i dati sanitari nel contesto emergenziale senza derogare alle normative nazionali e sovranazionali, appare necessario fare in questa sede una analisi doverosa.

Innanzitutto, va detto che l'Autorità Garante della privacy nel comunicato del 2 marzo 2020 ([123]) ha raccomandato che l'acquisizione di

([122]) F. PERRONE, *Questioni di conformità del diritto alla privacy dell'emergenza con il diritto dell'Unione Europea*, in *Diritto delle relazioni industriali*, Milano, Giuffrè, 1/6/2020.
([123]) Garante per la Protezione dei Dati Personali*, Coronavirus*, *no a iniziative "fai da te" nella raccolta dei dati. Soggetti pubblici e privati devono attenersi alle indicazioni del*

informazioni rilevanti ai fini della prevenzione e della diffusione del virus sia effettuata da soggetti che istituzionalmente esercitino queste funzioni in modo qualificato, quali gli operatori sanitari e il sistema attivato dalla protezione civile, ed ha richiamato i datori di lavoro ad "astenersi dal raccogliere, a priori e in modo sistematico e generalizzato, anche attraverso specifiche richieste al singolo lavoratore o indagini non consentite, informazioni sulla presenza di eventuali sintomi influenzali del lavoratore e dei suoi contatti più stretti o comunque rientranti nella sfera extra lavorativa".

Volendo verificare la compatibilità delle misure restrittive della privacy e della protezione dei dati personali di chi lavora in azienda, vanno citate le seguenti norme di riferimento, che indubbiamente, offrono la base giuridica del trattamento insita nella normativa emergenziale. Iniziando dalla normativa sovranazionale il considerando 46 del GDPR esplicita che "alcuni tipi di trattamento dei dati personali possono rispondere sia a rilevanti motivi di interesse pubblico sia agli interessi vitali dell'interessato, per esempio se il trattamento è necessario a fini umanitari, tra l'altro per tenere sotto controllo l'evoluzione di epidemie e la loro diffusione". Parallelamente, il considerando 52, relativo al trattamento di "categorie particolari di dati personali", richiama l'interesse pubblico, le finalità di sicurezza sanitaria, prevenzione o controllo di malattie trasmissibili e altre minacce gravi alla salute come basi giuridiche legittimanti il trattamento.

Va evidenziato che i considerando 46 e 52 vanno esaminati in relazione alla disciplina contenuta nell'art. 9 del GDPR, che, oltre a richiedere il consenso esplicito dell'interessato (par. 2 lettera a), in "materia di diritto del lavoro" al par. 2 lettera b) deroga al generale divieto di trattamento delle categorie particolari di dati proprio nel caso in cui il trattamento sia necessario per assolvere gli obblighi del titolare del trattamento, a condizione che il

Ministero della salute e delle istituzioni competenti, Nota del 2 marzo 2020 in www.garanteprivacy.it.

trattamento sia autorizzato dal diritto dell'Unione, o dal diritto degli Stati membri, ovvero in alternativa, da un contratto collettivo che assicuri garanzie appropriate per i diritti fondamentali e gli interessi del lavoratore.

L'art. 9 del GDPR, nel contesto lavorativo, stabilisce che il trattamento di dati sanitari può essere necessario per proteggere gli interessi vitali dell'interessato (par. 2 lettera c) e sottolinea inoltre la necessità di fronteggiare motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri (par. 2 lettera g). Sempre l'art. 9 considera, tra le norme rilevanti la necessità di trattare i dati per finalità di medicina preventiva o di medicina del lavoro, per la valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale (par. 2 lettera h). Infine, stabilisce che il trattamento dei dati personali sanitari può essere necessario per motivi di interesse pubblico rilevante nel settore della sanità pubblica (par. 2 lettera i).

Passando dalla normativa sovranazionale alla normativa interna, sempre allo scopo di ricercare le condizioni di liceità del trattamento dei dati sanitari in situazione emergenziale, e ricordando che il consenso dell'interessato è misura debole in ambito lavoristico, presupponendo una situazione di vera parità tra le parti difficilmente rintracciabile in tale contesto, vanno tenuti in debito conto almeno due ulteriori riferimenti normativi.

L'art. 5 dello Statuto dei lavoratori (da integrarsi con la disciplina di cui al d.lgs. n 81/2008 in materia di sicurezza sul lavoro) che vieta accertamenti da parte del datore di lavoro sulla idoneità e sulla infermità per malattia o infortunio, pur ammettendo che il controllo delle assenze per infermità possa essere effettuato soltanto attraverso i servizi ispettivi degli istituti previdenziali competenti. Va detto che non vi è traccia di alcuna norma, al momento, né nel Protocollo, né nella normativa approvativa dello stesso (d.l. 25 marzo 2020 n. 19 e successivi d.p.c.m. da esso richiamati) che demandi al

datore di lavoro alcun potere autonomo di introdurre provvedimenti attuativi delle misure di contenimento, né il legislatore ha introdotto alcuna deroga ai principi generali di cui all'art. 5 dello Statuto ed al d.lgs. 81/2008 ([124]).

Inoltre, va considerato l'art. 2087 c.c. che, come noto, obbliga il datore di lavoro ad assumere provvedimenti di controllo, effettuati nel rispetto della vigente normativa, finalizzati alla protezione della sicurezza dei lavoratori.

Pertanto, si può osservare che in virtù del Protocollo condiviso tra Governo e sindacati e sulla base della normativa europea e nazionale sopra riepilogata, è ammissibile il trattamento dei dati personali sanitari senza ledere il lavoratore sotto il profilo della tutela della sua riservatezza nonostante l'evidente impatto scaturente dalle nuove misure emergenziali. Ciò non esclude, però, che il datore di lavoro, anche nel contesto dell'emergenza sanitaria, sarà comunque tenuto ad agire secondo il principio dell'*accountability* (principio della responsabilizzazione) imposto dal GDPR e ad osservare tutti gli altri principi cardine in esso enunciati quali quello della proporzionalità, della minimizzazione e riservatezza dei dati personali.

([124]) A. SITZIA, *Coronavirus, controlli e "privacy" nel contesto del lavoro*, in *il Lavoro nella giurisprudenza*, Milano, IPSOA, 2020.

4.2 Le indicazioni dei Garanti privacy europei sul trattamento dei dati sanitari in emergenza

Le Autorità Garanti della maggior parte dei Paesi membri dell'Unione Europea hanno fornito una serie di linee guida volte a focalizzare l'attenzione degli operatori sugli aspetti fondamentali della disciplina emergenziale in materia di protezione dei dati personali nel suo bilanciamento con il diritto alla protezione della salute e della libertà d'impresa.

Va anzitutto ricordato che il 19 marzo 2020 è stata adottata la Dichiarazione ([125]) dell'*European Data Protecion Board* sul trattamento dei dati personali nel contesto dell'epidemia da COVID-19. Si tratta di una dichiarazione adottata dal Comitato europeo per la protezione dei dati, e cioè di un organo europeo indipendente che contribuisce all'applicazione coerente delle norme sulla protezione dei dati in tutta l'Unione Europea, ed è composto da rappresentanti delle Autorità nazionali per la protezione dei dati e dal Garante europeo della protezione dei dati.

La predetta dichiarazione anzitutto premette che è "nell'interesse dell'umanità arginare la diffusione delle malattie e utilizzare tecniche moderne nella lotta contro i flagelli che colpiscono estese aree del mondo", ricordando però "che qualsiasi misura adottata in questo contesto deve rispettare i principi generali del diritto e non può essere irrevocabile" in quanto le limitazioni della libertà sono legittime solo se "proporzionate e confinate al periodo di emergenza".

Nel contesto lavorativo il Comitato europeo per la protezione dei dati sottolinea che è particolarmente pertinente l'applicazione dei principi di proporzionalità e di minimizzazione dei dati, e che "il datore di lavoro

([125]) European Data Protecion Board, Dichiarazione sul trattamento dei dati personali nel contesto dell'epidemia da COVID-19, in www.edpb.europa.eu, 20/3/2020.

dovrebbe chiedere informazioni sanitarie soltanto nella misura consentita dal diritto nazionale" e che "dovrebbero accedere ai dati sanitari e trattarli solo se ciò sia previsto dalle rispettive norme nazionali". Infine, si richiede ai datori di lavoro di informare il personale sui casi di COVID-19 senza comunicare più informazioni del necessario, e qualora occorra indicare i nominativi dei dipendenti che hanno contratto il virus, i dipendenti interessati dovranno essere informati in anticipo con l'obiettivo di tutelare la loro dignità e integrità.

Per un rapido ed essenziale excursus sulle indicazioni dei tre più importanti Garanti privacy europei sul trattamento dei dati dei lavoratori in emergenza sanitaria, va citata la *Commission Nationale de l'informatique et des libertès* (CNIL) ([126]), l'autorità garante francese, che, tra l'altro, ha ritenuto non ammissibile la possibilità di rilevare la temperatura corporea di ciascun dipendente, agente o visitatore, o ancora, la registrazione di questionari o modelli medici.

Per quanto riguarda le indicazioni fornite dalla autorità tedesca, ossia *l'Office of the Federal Commissioner for Data and Freedom of Information* ([127]), il trattamento dei dati, anche sanitari, deve servire a prevenire o contenere al meglio la diffusione del virus tra i dipendenti e, pertanto, il trattamento può essere effettuato per ragioni di sicurezza quando è stata rilevata un'infezione o quando un dipendente ha preso contatto con una persona manifestamente infetta.

Il Garante spagnolo, *Agencia Espaniola de Proteccion de Datos* ([128]), sostiene invece che è essenziale individuare la base giuridica del trattamento tenendo conto del principio di minimizzazione, anche in relazione al

([126]) Commission Nationale de l'informatique et des libertès, *Coronavirus (COVID-19): les rappels de la CNIL sur la collecte de données personelles*, in www.cnil.fr, 6/3/2020.
([127]) Office of the Federal Commissioner for Data and Freedom of Information, in www.bfdi.bund.de, 7/2020
([128]) Agencia Espaniola de Proteccion de Datos, in www.aepd.es, 3/2020.

considerando 54 del GDPR. In sintesi, i datori di lavoro possono trattare i dati personali solo se adeguati, pertinenti e limitati a quanto necessario per impedire la diffusione del COVID-19.

È interessante osservare che, forse per la prima volta, l'Unione Europea, in forza di un evento emergenziale così rilevante come la pandemia, dà contemporaneamente attuazione alla normativa in materia di protezione dei dati e, ciascuna Autorità Garante, fornisce un proprio contributo nel solco di un obiettivo comune come quello del contrasto alla pandemia.

5. Trattamento dei dati sanitari, test diagnostici e vaccino anti COVID - 19: questioni e orientamenti del Garante privacy italiano

Ovviamente, anche l'Autorità Garante italiana si è espressa, a più riprese, sul trattamento dei dati particolari nell'emergenza sanitaria. A tal proposito, quello che qui soprattutto interessa è verificare quali siano le indicazioni sul trattamento di tali dati nel contesto lavorativo, e va detto che opportunamente il Garante ha messo a disposizione, di recente, le c.d. FAQ (Frequent Asked Questions) sui principali temi riguardanti il rapporto fra datore di lavoro e lavoratore in relazione alle principali situazioni che si possono verificare nella sede di lavoro nel contesto dell'emergenza sanitaria ([129]).

Ciò costituisce indubbiamente un aggiornamento in tempo reale, certificato dal Garante, delle modalità più consone di trattamento dei dati sanitari in ambito lavorativo. Qui di seguito, attraverso una disamina sintetica delle FAQ del Garante verranno riepilogate le questioni più attuali in materia di protezione dei dati sanitari, che costituiscono indubbiamente un "manuale di istruzioni" del Garante italiano per tutti gli operatori del settore.

Sulla rilevazione della temperatura corporea del personale dipendente, di utenti, fornitori, visitatori o clienti, qualora fosse associata all'identità dell'interessato, il Garante evidenzia che non è ammessa la registrazione del dato, bensì, nel rispetto del principio di minimizzazione è consentita la registrazione unicamente del superamento della soglia stabilita dalla legge e comunque quando sia necessario per documentare le ragioni che hanno impedito l'accesso al luogo di lavoro. Nel caso in cui la temperatura corporea venga rilevata a clienti (ad esempio nell'ambito della grande distribuzione),

([129]) Garante per la Protezione dei Dati Personali, FAQ sul Trattamento di dati nel contesto lavorativo pubblico e privato nell'ambito dell'emergenza sanitaria, www.garanteprivacy.it, 17/2/2020.

anche qualora la temperatura risulti superiore alla soglia, non è necessario registrare il dato relativo al motivo del diniego di accesso.

Il Garante sottolinea inoltre che il dipendente ha un obbligo specifico di segnalare al datore di lavoro qualsiasi situazione di pericolo per la salute e la sicurezza sui luoghi di lavoro, e il datore di lavoro può invitare i propri dipendenti a effettuare tali comunicazioni anche mediante canali dedicati. In ogni caso, in queste comunicazioni dovranno essere raccolti solamente i dati necessari, adeguati e pertinenti rispetto alla prevenzione del contagio ed il datore dovrà astenersi da richiedere informazioni aggiuntive in merito alla persona risultata positiva, alle specifiche località visitate, o altri dettagli relativi alla sfera privata.

Inoltre, In capo al medico competente permane, anche nell'emergenza, il divieto di informare il datore di lavoro circa le specifiche patologie sofferte dai lavoratori anche se dovrà segnalare al datore di lavoro situazioni di particolare fragilità e patologie attuali e pregresse dei dipendenti, suggerendo, eventualmente, l'impiego in ambiti meno esposti a rischi di infezione.

Il datore di lavoro, secondo le indicazioni del Garante non può comunicare il nome del dipendente che abbia contratto il virus a nessuno, ivi compresi i rappresentanti dei lavoratori per la sicurezza, con l'unica eccezione delle autorità sanitarie competenti, collaborando con le stesse per l'individuazione dei "contatti stretti" al fine di consentire la tempestiva applicazione delle misure di profilassi.

Il datore di lavoro può richiedere, poi, l'effettuazione di test sierologici solo se disposta dal medico competente, fermo restando che le informazioni relative alla diagnosi o alla anamnesi familiare del lavoratore non possono essere trattate dal datore di lavoro (ad esempio, mediante la consultazione dei referti o degli esiti degli esami). I datori di lavoro possono offrire ai propri dipendenti, anche sostenendone in parte o in tutto i costi, l'effettuazione di

test sierologici presso strutture sanitarie pubbliche e private, senza poter conoscere l'esito dell'esame.

Il Garante infine specifica che il datore di lavoro può trattare i dati relativi ai sintomi o alla positività al COVID-19 (identità del dipendente affetto da COVID-19 o che presenta sintomi compatibili con il virus, effettuazione di un tampone oro/nasofaringeo, avvenuta negativizzazione dello stesso tampone) 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.

In merito al trattamento dei dati relativi alla vaccinazione anti COVID-19 nel contesto lavorativo l'Autorità Garante ha voluto esemplificare tre situazioni particolari che possono verificarsi, vale a dire ([130]):

1) il datore di lavoro non può chiedere ai propri dipendenti di fornire informazioni sul proprio stato vaccinale, nemmeno sulla base del consenso dei dipendenti, non potendo il consenso costituire una valida condizione di liceità in ragione del più volte richiamato squilibrio dei rapporti tra titolare e interessato nel contesto lavorativo.

2) Il datore di lavoro non può chiedere al medico competente i nominativi dei dipendenti vaccinati, mentre potrà acquisire i soli giudizi di idoneità alla mansione specifica e le eventuali prescrizioni e/o limitazioni in essa riportati.

3) La vaccinazione anti COVID-19 dei dipendenti non può essere richiesta come condizione per l'accesso ai luoghi di lavoro e per lo svolgimento di determinate mansioni, atteso che al momento della definizione delle FAQ del Garante (febbraio 2021), non era entrata in vigore alcuna norma al riguardo. Conseguentemente, spetta al medico competente,

([130]) Garante per la Protezione dei Dati Personali, FAQ sul Trattamento di dati relativi alla vaccinazione anti COVID-19 nel contesto lavorativo, www.garanteprivacy.it, 17/2/2021.

trattare i dati personali relativi alla vaccinazione dei dipendenti e, se del caso, tenerne conto in sede di valutazione dell'idoneità alla mansione specifica.

Successivamente, con l'art. 4 del decreto legge n. 44 del 1/4/2021, in Gazzetta Ufficiale n. 79 del 1° aprile 2021 il legislatore ha introdotto l'obbligo di vaccinazione anti COVID-19 per "gli esercenti le professioni sanitarie e gli operatori di interesse sanitario che svolgono la loro attività nelle strutture sanitarie, socio sanitarie e socio-assistenziali, pubbliche e private, nelle farmacie e para farmacie e negli studi professionali." Con questa legge il legislatore ha inteso dare attuazione all'art. 32 della Costituzione, che, al secondo comma, prevede che "nessuno può essere obbligato a un determinato trattamento sanitario se non per disposizione di legge".

La legge prevede infatti, che: - il presupposto dell'obbligo vaccinale è che il vaccino anti COVID-19 è un requisito essenziale per l'esercizio della professione e per lo svolgimento delle prestazioni lavorative rese dai soggetti obbligati, tranne nel caso di accertato pericolo per la salute; - qualora il vaccino venga rifiutato l'azienda sanitaria locale ne dà comunicazione al datore di lavoro e all'ordine professionale di appartenenza con la conseguente sospensione del lavoratore dallo svolgimento di mansioni che implicano contatti interpersonali o comportano il rischio di diffusione del contagio; - il datore di lavoro, in tal caso verificherà se è possibile adibire il lavoratore ad altra mansione (anche inferiore) che non preveda l'esposizione al rischio; - qualora tale verifica desse esito negativo il datore di lavoro può sospendere il lavoratore senza retribuzione fino all'assolvimento dell'obbligo vaccinale e comunque non oltre il 31 dicembre 2021; - in caso di omissione o differimento della vaccinazione per ragioni mediche il datore di lavoro deve assegnare ai lavoratori interessati mansioni diverse senza riduzione della retribuzione.

Tre considerazioni possono farsi in relazione a questa legge introdotta di recente nel nostro Paese.

La prima è che non è stato introdotto un generale obbligo del vaccino anti COVID-19, ma con una norma specifica lo si è fatto solamente per il personale sanitario subordinato e autonomo, anche se il provvedimento solleva alcuni dubbi ([131]) su quali figure professionali siano destinatarie dell'obbligo vaccinale e se siano compresi i nuovi assunti e il personale assunto tramite contratti di somministrazione.

La seconda è che viene confermata la volontà del legislatore di escludere la sanzione del licenziamento in caso di rifiuto della vaccinazione.

La terza è che viene assegnato un ruolo decisivo all'autorità sanitaria locale nell'ambito della verifica dello stato vaccinale degli operatori sanitari e della conseguente sospensione dei lavoratori dalla prestazione lavorativa e dalla retribuzione ([132]).

Inoltre, da più parti in dottrina ([133]) è stato richiesto l'intervento del legislatore sulla questione della obbligatorietà del vaccino non solo per determinate categorie professionali, ma anche per la generalità degli individui; addirittura spingendosi a sostenere che quand'anche non vi fosse una legittimazione legislativa, l'obbligo di vaccinazione dovrebbe fondarsi su una legge morale, che dovrebbe essere insita in ogni individuo per orientare i comportamenti collettivi.

È ovvio che allo stato attuale la normativa sul tema è in continua possibile evoluzione, avendo riguardo sia agli sviluppi dell'emergenza sanitaria sia parallelamente agli sviluppi della campagna vaccinale in corso.

([131]) L. FAILLA, *Vaccino anti – COVID: obbligo solo per il personale sanitario. Tanti dubbi e qualche certezza*, in www.ipsoa.it, 15/5/2021.
([132]) F. D'AVANZO, *Vaccino anti COVID-19 obbligatorio per il personale sanitario*, in *Quotidiano giuridico*, Milano, UTET, 6/4/2021.
([133]) P. IERVOLINO, Vaccinazione e pandemia tra diritto ed etica, in Vaccinazione e rapporto di lavoro (a cura di) IERVOLINO, P., in *Lavoro e Previdenza Oggi*, 8/2/2012, www.rassegnadirittolavoro.it.

Il Ministero della Salute e il Ministero del Lavoro, il 6 aprile 2021 dopo un confronto con le Parti sociali hanno formalizzato il Protocollo ([134]) nazionale per la realizzazione dei piani aziendali finalizzati all'attivazione di punti straordinari di vaccinazione anti COVID – 19 nei luoghi di lavoro.

Il documento prevede che i costi per la realizzazione e la gestione dei siti previsti per la vaccinazione (inclusi i costi per la somministrazione), siano interamente a carico del datore di lavoro, mentre la fornitura dei vaccini, dei dispositivi per la somministrazione (siringhe/aghi) e la messa a disposizione degli strumenti formativi previsti e degli strumenti per la registrazione delle vaccinazioni eseguite è a carico dei Servizi Sanitari Regionali territorialmente competenti.

Alcuni elementi di interesse per quanto riguarda il trattamento dei dati sanitari vengono affrontati nel protocollo: il primo è che alle lavoratrici e ai lavoratori devono essere fornite tutte le necessarie informazioni con il necessario supporto del medico competente; le adesioni dei lavoratori interessati alla somministrazione del vaccino dovranno essere realizzate e gestite nel pieno rispetto della scelta volontaria evitando ogni forma di discriminazione; il medico competente assicura l'acquisizione del consenso informato del soggetto interessato e la tutela della riservatezza dei dati, assicurando la registrazione delle vaccinazioni eseguite mediante gli strumenti messi a disposizione dai Servizi Sanitari Regionali.

([134]) Protocollo nazionale per la realizzazione dei piani aziendali finalizzati all'attivazione di punti straordinari di vaccinazione anti COVID – 19 nei luoghi di lavoro del 6/4/2021 in ww.salute.gov.it

Bibliografia

ACHILLE, D., *Art. 5 Regolamento UE n. 2016/679 – Principi applicabili al trattamento di dati personali*, in BARBA, A., PAGLIANTINI, S., (a cura di), *Commentario del Codice civile – Delle persone – Leggi collegate Vol. II*, Milano, UTET Giuridica, 2019.

Agenzia dell'Unione Europea per i diritti fondamentali, Consiglio d'Europa, Garante europeo della protezione dei dati, (a cura di), *Manuale sul diritto europeo in materia di protezione dei dati*, Edizione 2018.

ALOVISIO, M., *Non viola la privacy la comunicazione dei dati sanitari del dipendente se è già resa nota dallo stesso*, in *Quotidiano Giuridico*, Milano, UTET, 15/9/2020.

ALVINO, I., *L'art. 4 dello Statuto dei lavoratori alla prova di internet e della posta elettronica*, in *Diritto delle relazioni industriali*, Milano, Giuffrè, 4/2014.

ASSONIME, nota n. 9 del 17/3/2020 – *Trattamento dei dati relativi a condanne penali e reati da parte delle imprese: verso l'attuazione dell'art. 2 - octies del Codice privacy* in www.assonime.it.

BARBA, A., PAGLIANTINI, S. (a cura di), *Commentario del Codice civile – Delle persone – Leggi collegate Vol. II*, Milano, UTET Giuridica, 2019.

BARBIERI, M., *L'utilizzabilità delle informazioni raccolte: il Grande Fratello può attendere (forse)*, in TULLINI, P., (a cura di) *Controlli a distanza e tutela dei dati personali del lavoratore*, Torino, Giappichelli, 2017.

BARRACO, E., SITZIA, A*., Potere di controllo e privacy. Ed. I*, Milano, IPSOA, 2016.

BELLAVISTA, A., *Il controllo sui lavoratori*, Torino, Giappichelli, 1995.

BELVEDERE, A., *Riservatezza e strumenti di informazione*, in *Dizionario del diritto privato*, Milano, Vallardi, 1980.

BENOCCHIO, G.A, CASUCCI F., (a cura di), *Temi e Istituti di Diritto Privato dell'Unione Europea*, Torino, Giappichelli, 2017.

BERNARDI, N., (a cura di) *Privacy. Protezione e trattamento dei dati*, Milano, IPSOA, 2019

BIANCA, F. *Art. 10 Regolamento UE n. 2016/679 – Trattamento di dati personali relativi a condanne penali e reati*, in BARBA, A., PAGLIANTINI, S. (a cura di), *Commentario del Codice civile – Delle persone – Leggi collegate Vol. II*, Milano, UTET Giuridica, 2019.

BOLOGNINI, L., PELINO, E., BISTOLFI, C. *Il Regolamento Privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali,* Milano, Giuffrè, 2016.

BOLOGNINI, L., *Regole nazionali e deontologiche per trattamenti nell'ambito del rapporto di lavoro*, in BOLOGNINI, L., PELINO, E., *Codice privacy: tutte le novità del d.lgs. n. 101/2018*, Milano, Giuffrè, 2018.

BRICOLA, F., *Prospettive e limiti della tutela penale della riservatezza*, in AAVV, *Il diritto alla riservatezza e la sua tutela penale*, Milano, Giuffrè, 1970.

CAIRO, L., VILLA, U*., I controlli a distanza a quattro anni dal Jobs Act*, Il *lavoro nella giurisprudenza*, Milano, IPSOA, 7/2019.

CATAUDELLA, A., *Art. 8* in PROSPERETTI, U., (diretto da), *Commentario dello Statuto dei lavoratori*, Milano, Giuffrè, 1975.

CATAUDELLA, A., *La tutela civile della vita privata*, Milano, Giuffrè, 1972.

CATAUDELLA, A., *Scritti giuridici*, Padova, CEDAM, 1991.

CECCHINATO, P. *In G.U. il D.lgs. n. 84/2020 che dà compiuta attuazione alla SHRD2*, in *Quotidiano giuridico*, Milano, UTET, 31/7/2020.

CIACCI, G*., Problemi e iniziative in tema di tutela dei dati personali con particolare riguardo ai dati sanitari*, in Politica del diritto, Bologna, Il Mulino, 1991.

CIVALE, F. *Requisiti e criteri di idoneità degli esponenti aziendali delle banche: prime riflessioni in margine al Decreto del MEF*, in www.dirittobancario.it, 21/12/2020.

CORTESI, M. F. *Prosegue il cammino della "riforma Orlando" anche in materia di casellario giudiziale*, in *Quotidiano giuridico*, Milano, UTET, 31/10/2018.

D'AVANZO, F., *Vaccino anti COVID-19 obbligatorio per il personale sanitario*, in *Quotidiano giuridico*, Milano, UTET, 6/4/2021.

DEL PUNTA, R., *Diritti della persona e contratto di lavoro* in *Giornale di diritto del lavoro e di relazioni industriali*, Milano, FrancoAngeli, 2006.

DEL PUNTA, R., SCARPELLI, F., *Codice commentato del lavoro, Ed. I*, Milano, IPSOA, 2019

DI CIOMMO, F., *La privacy sanitaria*, in PARDOLESI, R., (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, Giuffrè, 2003.

DI FEDERICO, G., NEGRI, S., *Unione Europea e salute*, Padova, CEDAM, 2020.

FAILLA, L., *Vaccino anti – COVID: obbligo solo per il personale sanitario. Tanti dubbi e qualche certezza*, in www.ipsoa.it, 15/5/2021.

FARALLI, C. *Il diritto alla privacy. Profili storico-filosofici*, in *Persona e mercato dei dati. Riflessioni sul GDPR* (a cura di) GALGANO, N., Padova, CEDAM, 2019.

FESTA, M., *Coronavirus: il Garante privacy si esprime sulla richiesta di parere chiesto dalla protezione civile, in Quotidiano Giuridico*, Milano, UTET, 14/2/2020.

FINOCCHIARO, G., *Introduzione al Regolamento europeo sulla protezione dei dati*, in *Nuove leggi civili commentate*, Padova, CEDAM, 1/2017.

FINOCCHIARO, G., *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Bologna, Zanichelli, 2012.

FOIS, S., *Questioni sul fondamento costituzionale del diritto alla "identità personale"*, in AAVV, *L'informazione e i diritti della persona*, Napoli, Jovene, 1983.

GRANIERI, M., *Il trattamento di categorie particolari di dati personali nel Reg. UE 2016/679*, in *Nuove leggi civili commentate*, Padova, CEDAM, 1/2017.

GRASSO, G., *Tutela della privacy e trattamento dei dati sensibili* in *Il libro dell'anno del diritto*, Roma, Istituto Enciclopedia Italiana, 2019.

IERVOLINO, P., *Vaccinazione e pandemia tra diritto ed etica, in Vaccinazione e rapporto di lavoro* (a cura di) IERVOLINO, P., in *Lavoro e Previdenza Oggi*, 8/2/2012, www.rassegnadirittolavoro.it.

JHERING, R., *Recthsschutz gegen injuriose Rechtsverletzungen*, in *Jahrbucher fur die Dogmatik des heutigen romischen und deutschen Privatrechts*, XXIII, 1885, citato in SIRENA, P., *Il sequestro della stampa a tutela del diritto all'immagine*, in *Studi in onore di Giovanni Giacobbe, Vol. II* (a cura di) G. DALLA TORRE, Milano, Giuffrè, 2010.

LAZZARI, C., *Le visite di pre-assunzione fra divieto di analogia, potenzialità discriminatorie e tutela della riservatezza*, in *Giurisprudenza Italiana*, 4/1999.

MARAGLINO, R. *Dati giudiziari, fermo al palo il trattamento per i lavoratori*, in www.agendadigitale.eu, 31/10/2019.

MARAZZA, M., *I controlli a distanza del lavoratore di natura "difensiva"*, in TULLINI, P., (a cura di) *Controlli a distanza e tutela dei dati personali del lavoratore*. Torino, Giappichelli, 2017.

MARTORANA, M., TESORO, A., *Le informazioni da fornire all'interessato e le modalità di raccolta del consenso ai sensi del d.lgs. 101/2018* in MARTORANA, M., (a cura di) *GDPR e decreto legislativo 101/2018*, Padova, CEDAM, 2019.

MAZZARO, A., MAZZONE, D., *GDPR e rapporto di lavoro,* Milano, Giuffrè, 2020.

MENGONI, L., *Introduzione al titolo I, in Commentario dello Statuto dei lavoratori* diretto da PROSPERETTI, U., Milano, Giuffrè, 1975.

MIRONE, M*., Il dato personale: cos'è e come trattarlo*, in MARTORANA, M., (a cura di) *GDPR e decreto legislativo 101/2018*, Padova, CEDAM, 2019.

MONEA, A., *Trattamento dei dati lavorativi e protezione dei dati personali nell'ente locale*, in *Azienditalia*, Milano, IPSOA, 11/2018.

MONTEMEZZO, L., *La sorveglianza sanitaria dei lavoratori: fra tutela della salute e protezione della privacy,* in www.buttiandpartners.com, 23/10/2019.

PASCUCCI, P., DELOGU, A., *Salute e sicurezza nei luoghi di lavoro, in Diritto e processo del lavoro e della previdenza sociale*, *Tomo secondo*, SANTORO-PASSARELLI, G. (a cura di), Milano, UTET, 2020.

PEDRAZZI, G., *Art. 88 Regolamento UE n. 2016/679 – Trattamento dei dati nell'ambito dei rapporti di lavoro*, in BARBA, A., PAGLIANTINI, S. (a cura di), *Commentario del Codice civile – Delle persone – Leggi collegate Vol. II*, Milano, UTET Giuridica, 2019.

PELLECCHIA, E. *Profilazione e decisioni automatizzate al tempo della Black Box Society: qualità dei dati e eleggibilità dell'algoritmo nella cornice della responsabile research and innovation,* in *Nuove Leggi Civili Commentate*, Padova, CEDAM, 2018.

PERRONE, F., *Questioni di conformità del diritto alla privacy dell'emergenza con il diritto dell'Unione Europea*, in *Diritto delle relazioni industriali*, Milano, Giuffrè, 1/6/2020.

PEZZUTO, A. *Nuovi requisiti e criteri di idoneità degli esponenti aziendali*, in *Rivista di diritto bancario e finanziario Tidona*, www.tidona.com, 12/1/2021.

PIZZETTI, F., *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo, Vol. I*, Torino, Giappichelli, 2016.

PIZZOFERRATO, A., *Gli effetti del GDPR sulla disciplina del trattamento aziendale dei dati del lavoratore*, in *Argomenti di Diritto del Lavoro*, Milano, La Tribuna, 4-5, 2018.

PIZZORUSSO, A., *I profili costituzionali di un nuovo diritto della persona*, in AAVV, *Il diritto alla identità personale*, (a cura di) ALPA, G., BESSONE, M., Padova, CEDAM, 1981.

PROIA, G., Manuale di diritto del lavoro, Ed. III, Padova, CEDAM, 2020.

RESCIGNO, P., *Il diritto all'identità della vita privata, in studi in onore di F. Santoro Passarelli, IV*, Napoli, Jovene, 1972.

RESTA, F., *Art. 5 in GDPR e normativa privacy*, (a cura di) RICCIO, G.M., SCORZA, G., BELLISARIO, E., Milano, IPSOA, 2018.

RODOTÀ, S., *Riservatezza*, in *Enciclopedia Italiana*, VI Appendice, Istituto della enciclopedia italiana, Treccani, 2000.

RUSSO, M. *Richiesta del certificato penale e del certificato carichi pendenti ai fini della assunzione*, in www.ilgiuslavorista.it, 2/7/2019.

SANTONI, F., *La privacy nel rapporto di lavoro: dal diritto alla riservatezza alla tutela dei dati personali*, in TULLINI, P., *Tecnologie della comunicazione e riservatezza nel rapporto di lavoro*, Padova, CEDAM, 2010

SCHIAVONE, R. *Nuovo codice privacy e gestione del rapporto di lavoro,* in *Il lavoro nella giurisprudenza*, Milano, IPSOA, 2018.

SITZIA, A., *Coronavirus, controlli e "privacy" nel contesto del lavoro*, in *il Lavoro nella giurisprudenza*, 5, Milano, IPSOA, 2020.

STENICO, E., *Il trattamento dei dati personali del lavoratore subordinato: dalla segretezza al controllo*, in *Quaderni di diritto del lavoro e relazioni industriali*, Milano, UTET, n. 24, 2000.

TUCCILLO, R. *Art. 9 Regolamento UE n. 2016/679 – Trattamento di categorie particolari di dati personali*, in BARBA, A., PAGLIANTINI, S., (a cura di), *Commentario del Codice civile – Delle persone – Leggi collegate Vol. II*, Milano, UTET Giuridica, 2019.

TULLINI, P., (a cura di) *Controlli a distanza e tutela dei dati personali del lavoratore*. Torino, Giappichelli, 2017.

VALENTI, A.M., *La dignità umana quale diritto inviolabile dell'uomo*: *luci ed ombre nelle moderne esperienze internazionali e bioetiche nell'approssimarsi del terzo millennio*, Perugia, Università di Perugia, 1995.

WARREN, S., BRANDEIS, L., *The right to privacy*, in *4 Harvard Law Review*, 1890 – 1891.

Giurisprudenza e normativa

Agencia Espaniola de Proteccion de Datos, in www.aepd.es, 3/2020.

Cass. 17/7/2007 n. 15892 in *Rivista Italiana di Diritto del Lavoro*, Milano, Giuffrè, 714, 2008, con nota di M. VALLURI.

Cass. 19/1/2002, n. 570 in *Rivista Italiana di Diritto del Lavoro*, Milano, Giuffrè, 511, 2002.

Cass. 28/3/1984, n. 2052 in *Foro italiano*, 1984.

Cass. Sez. I civ. Ordinanza 16560/2020 in Diritto e Giustizia, 3/8/2020.

Cass. SU 27/12/2017 n. 3098 in *Foro italiano*, I, 2147, 2018.

Cass., sent. 27/5/1975, n.2129 in *Foro italiano*, I, 1976.

Cass. sez. lav., sent. 17/7/2018 n. 19012 in www.dirittoegiustizia.it, 18/7/2018.

Commission Nationale de l'informatique et des libertès, *Coronavirus (COVID-19) : les rappels de la CNIL sur la collecte de donnèes personelles*, in www.cnil.fr, 6/3/2020.

Consiglio d' Europa, Convezione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, Strasburgo, 28/1/1981.

Corte Cost., sent. 12/4/1973 n.38 in *Gazzetta Ufficiale* n. 102, 18/4/1973.

Decreto legislativo 9/4/2008 n. 81, Attuazione dell'art. 1 della legge 3 agosto 2007 n. 123, in materia di tutela della salute e della sicurezza nei luoghi di lavoro, in *Gazzetta Ufficiale* n. 101 del 30/4/2008.

Delibera del Consiglio dei ministri 31/1/2020, Dichiarazione dello stato di emergenza in conseguenza del rischio sanitario connesso all'insorgenza di patologie derivanti da agenti virali trasmissibili, in *Gazzetta Ufficiale* n. 26 dell'1/2/2020.

Direttiva 2013/36/UE del Parlamento europeo e del Consiglio del 26/6/2013, in *Gazzetta Ufficiale dell'Unione Europea*, 27/6/2013.

Direttiva 81/1981 del Comitato dei Ministri del Consiglio d'Europa relativa alla regolamentazione applicabile alle banche di dati sanitari automatizzate, in www.privacy.it, 23/1/1981.

Direttiva 95/46/CE del Parlamento europeo e del Consiglio, 24/10/1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati in Gazzetta ufficiale delle Comunità europee del 23/11/1995.

European Data Protecion Board, Dichiarazione sul trattamento dei dati personali nel contesto dell'epidemia da COVID-19, in www.edpb.europa.eu, 20/3/2020.

Garante per la Protezione dei Dati Personali, Autorizzazione n. 7/2016 al Trattamento di dati giudiziari da parte di privati, di enti pubblici economici e di soggetti pubblici, in *Gazzetta Ufficiale* n. 303 del 29/12/2016.
Garante per la Protezione dei Dati Personali, Provvedimento n. 314 del 22/6/2018, Doc. web n. 9005845.

Garante per la Protezione dei Dati Personali, Provvedimento del 19/7/2018 in tema di Autorizzazioni generali del Garante per la protezione dei dati personali, Doc. web n. 9026901.

Garante per la Protezione dei Dati Personali, Provvedimento del 4/12/2019, Doc. web n. 9215890.

Garante per la Protezione dei Dati Personali, Provvedimento correttivo e sanzionatorio nei confronti di Tim S.p.A., Doc. web n. 9263597, 9/1/2020.

Garante per la Protezione dei Dati Personali, FAQ sul Trattamento di dati nel contesto lavorativo pubblico e privato nell'ambito dell'emergenza sanitaria, garanteprivacy.it, 17/2/2020.

Garante per la Protezione dei Dati Personali, FAQ sul Trattamento di dati relativi alla vaccinazione anti COVID-19 nel contesto lavorativo, www.garanteprivacy.it, 17/2/2021.

Garante per la Protezione dei Dati Personali*, Coronavirus*, *no a iniziative "fai da te" nella raccolta dei dati. Soggetti pubblici e privati devono attenersi alle indicazioni del Ministero della salute e delle istituzioni competenti*, Nota del 2 marzo 2020 in www.garanteprivacy.it.

Gruppo di lavoro Art. 29, Linee Guida n. 260/2017 sul principio di trasparenza ai sensi del Regolamento n. 2016/679.

Gruppo di Lavoro Articolo 29 per la protezione dei dati, Parere 2 dell'8/6/2017 sul trattamento dei dati sul posto di lavoro, in www.privacy.it.

Interpello n. 4 del 28/5/2019 ai sensi dell'art. 12 del d.lgs. n. 81/2008 e successive modificazioni-Tenuta della documentazione sanitaria su supporto informatico, in www.lavoro.gov.it

Office of the Federal Commissioner for Data and Freedom of Information, in www.bfdi.bund.de, 7/2020.

Pretura Milano, 27/2/1975, in *Rivista Italiana di Diritto del Lavoro*, Milano, Giuffrè, II, 882, 1975.

Pretura Milano, 10/12/1974, in *Rivista Italiana di Diritto del Lavoro*, Milano, Giuffrè, II, 236, 1977.

Protocollo condiviso di regolamentazione delle misure per il contrasto e il contenimento della diffusione del virus COVID-19 negli ambienti di lavoro, del 14/3/2020, successivamente integrato il 24/4/2020, in allegato 12 al D.p.c.m 3/12/2020, in *Gazzetta Ufficiale*, n. 301, 3/12/2020, aggiornato e rinnovato il 6/4/2021 in www.salute.gov.it.

Protocollo nazionale per la realizzazione dei piani aziendali finalizzati all'attivazione di punti straordinari di vaccinazione anti COVID – 19 nei luoghi di lavoro del 6/4/2021 in ww.salute.gov.it.

Senato della Repubblica, V legislatura, Doc. n. 738, 2, 1969.