EMERGENZA CORONAVIRUS E PROTEZIONE DEI DATI PERSONALI DEL LAVORATORE

CAPITOLO III

SMART WORKING: CONCILIARE, INNOVARE E COMPETERE

UNO STRUMENTO PER LA GESTIONE DELL' EMERGENZA

CAPITOLO IV

EMERGENZA PANDEMICA E PROCESSO DI ADEGUAMENTO DELLE IMPRESE

INTRODUZIONE

La recente emergenza sanitaria ha reso evidente la necessità di regolamentare il delicato rapporto intercorrente tra protezione dei dati e tutela della salute pubblica, imponendo attente riflessioni in relazione agli strumenti e garanzie da adottare nel rapporto di lavoro.

La pandemia, legata alla diffusione del COVID-19 è stata un banco di prova importante sotto molti profili, la privacy è stato uno di essi. Su questo terreno si è, infatti riproposto il conflitto, dalle antiche radici, tra persona e Stato, libertà e autorità, norma ed emergenza, in forme rese del tutto inedite e più complesse nei termini di questo rapporto. Come indicato dal nuovo Presidente dell'Autorità Garante per la protezione dei dati personali Prof. Pasquale Stanzione "… In un contesto così difficile, in cui era ricorrente l'invocazione del "*necessitas non habet legem*", la disciplina privacy ha, dimostrato una straordinaria resilienza, indicando come coniugare riservatezza individuale ed esigenze di sanità pubblica, realizzando quel bilanciamento tra salute e dignità voluto da Aldo Moro nell' art. 32 della Costituzione". La forza della privacy si è rilevata, paradossalmente, proprio la sua "mitezza" (*Gustavo Zagrebelsky*), la sua capacità, cioè, di ammettere limitazioni alla pienezza del suo esercizio purché strettamente indispensabili al perseguimento di un fine di preminente interesse generale quale il contenimento dei contagi"[1]. Le emergenze limitano tutte le libertà, basti pensare al blocco della libera circolazione su scala nazionale adottato nella fase acuta emergenziale, ed una compressione delle libertà così forte nel nostro paese, è risultata senza precedenti in tempi di pace e quindi per il diritto alla protezione dei dati personali ed alla privacy, un diritto di libertà.

La privacy è un diritto fondamentale, per sua natura, dai costituzionalisti definito non tiranno, quindi soggetto a bilanciamenti con altri beni giuridici come la salute pubblica.

L'emergenza è in realtà una condizione giuridica che legittima in generale le limitazioni della libertà, purché proporzionali alle esigenze di contrasto e temporalmente limitate al protrarsi dello stato di gestione. Le Autorità della salute pubblica e la Direzione della Protezione civile in stretta connessione con l'Autorità Garante della Privacy in forte interlocuzione hanno operato al fine di perseguire questo bilanciamento. Seguendo la logica dell' analisi dei rischi, il rischio è appunto definire meccanismi non proporzionati, che delineino il se ma anche il come, per la limitazione di questi diritti, con controlli, tracciamenti, ed avendo cura di evitare scelte irreversibili e/o iniziative fai da sé[2], rimandando all' assunzione di responsabilità di chi ha titolo, quali le Autorità e la Protezione civile che sono forti di poteri delegati, e non quindi a chiunque, quali aziende e datori di lavoro come nel caso della misurazione delle temperature all' ingresso dei lavoratori, scelte da fare sempre in ossequio

[1] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9442541

[2] https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9265883

a garanzie minime ed imprescindibili in termini di conservazione e nel rispetto delle finalità dichiarate. Si tratta quindi di ricondurre le scelte emergenziali in una cornice costituzionale compatibile e senza perdere di vista l'obiettivo: la ricostruzione della catena epidemiologica efficace per il contrasto della diffusione del virus.

Il nostro ordinamento, che a differenza di altri, non ammette un regime "*extra ordinem*" per lo stato di eccezione, norma con adeguate garanzie anche l'emergenza, e contempla quest'ultima non come fonte del diritto ma quale circostanza da ascrivere in un quadro di garanzie costituzionali con tutte le deroghe del caso.

Riferimenti fondamentali sono in un tale contesto fonti aperte, dati anonimi e aggregati, dati conservati per intervalli di tempo limitati e che non escano dai dipartimenti degli atenei in caso di sperimentazioni. Uno dei punti di maggiore criticità è proprio il monitoraggio dei contatti dei casi positivi: per attivarlo e andare a indagare sulla posizione e sugli spostamenti dei singoli cittadini e delle persone che incrociano, seppur ridistribuendoli anonimamente, nel rispetto di regole e garanzie, come sottolineato anche dall' *European Data Protection Board* citando il Regolamento europeo per la privacy GDPR, che consente il trattamento per finalità di sicurezza nazionale ma allo stesso tempo richiede una valutazione d'impatto e sulla sicurezza.

Sul tracciamento dei contagi anche in Italia, risulta fondamentale il parere dell'Autorità GARANTE[3]: *"L'acquisizione di trend, effettivamente anonimi, di mobilità potrebbe risultare una misura più facilmente percorribile, laddove, invece, si intendesse acquisire dati identificativi, sarebbe necessario prevedere adeguate garanzie, con una norma ad efficacia temporalmente limitata e conforme ai principi di proporzionalità, necessità, ragionevolezza. In tal senso, andrebbe effettuata un'analisi dell'effettiva idoneità della misura a conseguire risultati utili nell'azione di contrasto. Ad esempio, apparirebbe sproporzionata la geolocalizzazione di tutti i cittadini italiani, 24 ore su 24, non soltanto per la massività della misura ma anche e, forse, preliminarmente, perché non esiste un divieto assoluto di spostamento e dunque la mole di dati così acquisiti non avrebbe un'effettiva utilità. Diversa potrebbe essere, invece, la valutazione relativa alla geolocalizzazione, quale strumento di ricostruzione della catena epidemiologica. In ogni caso, è indispensabile una valutazione puntuale del progetto. Non è il tempo dell'approssimazione e della superficialità".*

La materia della protezione dei dati è stata definita un "diritto inquieto" poiché in dialettica con una tecnica in continua evoluzione e con i molteplici interessi, di natura sia individuale che collettiva, ma che trova forza nella sua funzione sociale: nel contrasto al virus essa si rivela, allora,

[3] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9296264

indispensabile “rappresentando il punto di equilibrio tra libertà e tecnica, tra persona e società, il presupposto della tenuta della democrazia anche in circostanze eccezionali”.

Anche il Comitato europeo per la protezione dei dati ha affermato che non dovrebbe esserci una scelta tra risposta efficace alla crisi e la tutela dei diritti fondamentali, essendo possibile realizzare entrambi gli obiettivi: “i principi di protezione dei dati possono svolgere un ruolo molto importante nella lotta contro il virus” dal momento che “il diritto europeo in materia di protezione dei dati consente l’uso responsabile dei dati personali per la gestione della salute, garantendo al contempo che non siano erosi i diritti e le libertà individuali.

Nelle pagine che seguono si sono analizzati i principali impatti tra la gestione dell’Emergenza COVID-19 e la protezione dei dati personali e, nello specifico, nel rapporto lavoratore azienda. Nel primo capitolo si è ricostruita sinteticamente l’evoluzione della normativa comunitaria e nazionale sulla protezione delle informazioni e dei dati personali in relazione all’ emergenza COVID-19. Nel secondo capitolo viene fornita una breve panoramica del quadro normativo di riferimento ed i suoi aggiornamenti specificatamente all’ emergenza COVID-19. Nella seconda parte del capitolo stesso si presentano le peculiarità degli interventi normativi emergenziali con impatti sulla protezione dati dei lavoratori. Raccolta delle principali disposizioni adottate in relazione allo stato di emergenza epidemiologica da COVID-19 aventi implicazioni in materia di protezione dei dati personali. I due capitoli successivi (terzo e quarto) entrano nel vivo della questione. In essi viene dapprima presentato nel capitolo terzo, il modello “*SMART WORKING*”, quale modello principe, in questa situazione emergenziale, ove applicabile, per conciliare, innovare e competere. In particolare, nel quarto capitolo vengono illustrati i criteri da seguire e gli strumenti utilizzati nel processo di adeguamento delle imprese in modo da garantire un sistema di sicurezza che fosse conforme alle disposizioni in materia di protezione dati e privacy nella gestione dell’emergenza COVID-19.

In conclusione, si vuole fornire degli elementi critici di valutazione in relazione al contesto normativo, situazione emergenziale e protezione dei dati personali. Le questioni attinenti alla proprietà delle informazioni e dei dati personali del lavoratore, alle modalità di accesso alle stesse sono, infatti sempre più condizionanti l’efficienza e la produttività delle aziende. Come testimonia lo sviluppo stesso della digitalizzazione, l’accento si è spostato dai mezzi di trasmissione ai contenuti informativi.

Lo studio che segue si propone di evidenziare soprattutto l’importanza di una legge che disciplina l’accesso e l’utilizzo dei dati relativi alle persone che hanno relazioni con le aziende in modo diretto ed indiretto, che siano dipendenti aziendali o clienti finali, per ridurre il rischio di un uso improprio, se non criminale, dei dati che contribuiscono a definire il “profilo del lavoratore”.

CAPITOLO I
LA NORMATIVA COMUNITARIA E NAZIONALE SULLA PROTEZIONE DELLE INFORMAZIONI E DEI DATI PERSONALI

1. Premessa

Unitamente alle problematiche connesse alla diffusione delle nuove tecnologie, hanno iniziato ad assumere un rilievo sempre maggiore gli istituti del diritto che tutelano l'uomo sia nella sua dimensione individuale che in quella collettiva. A partire, infatti, dalla diffusione delle prime banche dati, è emersa con vigore l'esigenza di tutelare la persona e la sua riservatezza contro l'indiscrezione da parte di terzi nella sfera della vita privata. In un primo momento il campo della privacy appare sostanzialmente legato all' idea dell'inviolabilità del domicilio[4] e della corrispondenza, come espressione dei luoghi e dei momenti in cui rilevare l'intimità degli individui[5]. Solo recentemente, nell' era informatica, si delinea la necessità di tutelare, oltre alla riservatezza, la dignità e l'identità personale e quindi ogni dato che in relazione ad altri, permetta di identificare una persona. Pietra miliare nell' elaborazione normativa in tema di dati personali è la Convenzione n.108 di Strasburgo, approvata dal Consiglio d' Europa il 22 settembre 1980 e riguardante la protezione della persona rispetto al trattamento automatizzato di dati di carattere personale[6]. Lo scopo della Convenzione risiede nella garanzia del rispetto dei diritti e delle libertà fondamentali di ciascuno, in particolare il diritto alla vita privata, a prescindere dal luogo di cittadinanza o di residenza. Ogni stato membro, si impegna quindi, ad adottare nel proprio diritto interno le misure necessarie per controllare l'attività di raccolta, elaborazione e diffusione dei dati, dal momento che già diversi Paesi garantiscono i diritti della personalità in apposite disposizioni o nel proprio complesso ordinamento. I diritti della persona devono essere protetti a prescindere dalle frontiere, attenuando le diversità tra le legislazioni e prevenendo eventuali politiche protezionistiche.

La rilevanza del dato personale ed il suo conseguente trattamento giuridico divergono a seconda che si tratti di dati "sensibili", riguardanti l'intimità della vita privata (l'origine razziale, le opinioni politiche, le convinzioni religiose, la salute, la vita sessuale, etc.) e per i quali vige il divieto di elaborazione automatizzata, dati economici, inerenti alla sfera dell'iniziativa economica del soggetto e dati derivanti da fonti pubblicamente accessibili. I dati devono essere registrati per scopi determinati e legittimi, compatibilmente con le finalità che ne hanno giustificato la raccolta. La Convenzione

[4] BARILE P. - CHELI E. *Domicilio (libertà di),* in *Enciclopedia del Diritto, XIII*, 1964, pagg. 859-870. Il riconoscimento del nesso inscindibile tra persona e domicilio induce a ritenere che nella tutela del domicilio converge anche una tutela della sfera privata della persona. Si osserva infatti che nel domicilio l'ordinamento tutela la persona riflessa in una certa sfera spaziale volta a preservare il carattere intimo, domestico, o quantomeno privato di determinati rapporti soggettivi.

[5] CUFFARO V., RICCIUTO V., ZENO-ZENCOVICH V., *Trattamento dei dati e tutela della persona*, Milano, 1998, pag. 51 ss.

[6] BUTTARELLI G. - *Banche dati e tutela della riservatezza*, Milano 1997, pag. 8 ss. Nel preambolo si riafferma l'impegno del Consiglio d'Europa per la libertà di informazione senza considerazione di frontiere, e si riconosce la necessità di conciliarla con la vita privata. Ciò ha fatto ritenere che il fine della Convenzione non sia quello della tutela dei diritti, e consista nel porre alcuni principi per prevenire ostacoli al flusso internazionale dei dati.

riconosce, inoltre alla persona cui i dati si riferiscono, alcune garanzie minime che le consentano di esercitare un controllo sull' attività di raccolta, elaborazione e diffusione dei dati, senza per questo limitare ciascuno Stato nell' accordare alle persone cui questi si riferiscono, una protezione più vasta di quella prevista dalla Convenzione stessa estendendo ad esempio l'efficacia dei principi di quest'ultima alle persone giuridiche ed agli enti di fatto.

Il trattamento di tutti questi dati, se vietato, talvolta a livello costituzionale è consentito qualora l'ordinamento interno preveda garanzie adeguate: alcuni Paesi; quindi, lo considerano lecito solo se effettuato in forma anonima e a fini statistici, mentre altri richiedono comunque il preventivo consenso espresso o formale dell'interessato. Non di rado, poi, si prevede un'autorizzazione o un parere preliminare di un'autorità di controllo, oltre ad ulteriori adempimenti che il legislatore consente di adottare, ad esempio in via amministrativa o regolamentare. È importante, inoltre, l'articolo 12 della Convenzione che disciplina il movimento oltrefrontiera di qualunque categoria di dati personali, a prescindere dal sistema di trasmissione, dal supporto utilizzato e dalle relazioni soggettive tra mittente e destinatario. Al principio del libero flusso, il paragrafo 3 sancisce due deroghe riguardanti la prima il diritto interno, circa una disciplina particolare per talune categorie di dati o di banche dati, la seconda le ipotesi in cui il flusso dei dati sia diretto apparentemente verso una Parte, ma abbia come effettiva destinazione, per il tramite di essa, un paese terzo non contraente.

La Convenzione disciplina anche la cooperazione tra le Parti, dovendo ciascuno Stato designare una o più autorità che collaborino tra loro scambiandosi informazioni giuridiche e controllando anche in via preliminare le elaborazioni automatizzate. È fondamentale l'importanza di questo documento che ha avuto un ruolo propulsivo e che contiene, come abbiamo visto i principi fondamentali recepiti da altri dettati normativi, che hanno contribuito a delineare quanto la spinta verso la globalizzazione abbia posto questioni rilevanti in termini di riservatezza.

2. La normativa comunitaria ante GDPR

La Direttiva 95/46/CE "La tutela delle persone fisiche con riguardo al trattamento dei dati e alla loro libera circolazione" è il massimo comune denominatore europeo al quale si sono dovute adeguare tutte le leggi straniere, presenta alcuni tratti originali, configurando una nuova disciplina del trattamento dei dati personali. Essa rende esplicita, come dallo stesso titolo si può osservare, l'esigenza di contemperare due interessi specificatamente coinvolti: la tutela delle persone fisiche e la libera circolazione dei dati. Lo scopo della Direttiva risiede nella creazione di "uno spazio senza frontiere interne" nella circolazione delle merci, delle persone, dei servizi e dei capitali, consentendo in questo modo anche l'abbassamento dei costi delle imprese. La Direttiva prende in considerazione solo i dati riferiti a persone fisiche, dovendo bilanciare le singole legislazioni nazionali degli Stati membri che in materia si presentano divergenti. La Direttiva definisce sia la procedura cui è tenuto il

responsabile del trattamento, considerando come tale qualsiasi operazione compiuta con o senza l'ausilio di processi automatizzati e riguardanti ogni fase che va dalla raccolta alla diffusione/comunicazione, sia i diritti della persona interessata, a cui si riferiscono i dati. A carico del responsabile, che è il centro di imputazione della responsabilità da trattamento dei dati e che non è distinto come figura dal titolare, sono previsti alcuni adempimenti, tra i quali la notifica del trattamento dei dati all'autorità di controllo nazionale e la richiesta del consenso al trattamento dei dati.

I dati riconosciuti alla persona interessata dal responsabile del trattamento e che coincidono con quelli previsti dalla Convenzione di Strasburgo sono:

- La conferma dell'esistenza o meno di trattamenti di dati che la riguardano;
- La comunicazione dei dati che sono oggetto dei trattamenti e le informazioni sull'origine dei dati;
- La rettifica, la cancellazione o il congelamento nel caso in cui il trattamento non sia conforme alle disposizioni della Direttiva;
- La notifica ai terzi, ai quali i dati sono stati comunicati, dell'esecuzione di qualsiasi delle suddette operazioni.

Gli Stati membri riconoscono inoltre alla persona interessata il diritto di opporsi al trattamento di dati che la riguardano, nell'ipotesi in cui la legge non richieda il consenso, per motivi prioritari e legittimi o nel caso in cui il trattamento sia finalizzato all'invio di materiale pubblicitario. Per quanto riguarda specificatamente i dati "sensibili", la Direttiva vieta in via di principio il trattamento, ammettendolo solo con il consenso esplicito dell'interessato e per assolvere ad obblighi e diritti del responsabile del trattamento in materia del diritto del lavoro o per la salvaguardia di un interesse vitale[7]. È inoltre fondamentale, per la sicurezza dei trattamenti, che il responsabile attui misure tecniche ed organizzative appropriate al fine di garantire la protezione dei dati personali dalla distruzione o perdita accidentale o illecita, dalla diffusione o dall'accesso non autorizzato, soprattutto quando l'operazione comporta trattamenti di dati all'interno di una rete.

Per quanto riguarda il trasferimento di dati verso Paesi terzi, l'articolo 25 della Direttiva dispone che esso può aver luogo soltanto se viene garantito un livello di protezione adeguato e prevedendo sanzioni da applicare in caso di violazione delle disposizioni della Direttiva. Al riguardo, la norma prefigge ai legislatori nazionali una disciplina che preveda il diritto di "chiunque subisca un danno cagionato da un trattamento illecito…di ottenere il risarcimento da pregiudizio subito dal responsabile del trattamento", potendo quest'ultimo "essere esonerato in tutto o in parte da tale responsabilità se prova che l'evento dannoso non gli è imputabile".

[7] Cfr. Sezione III, art 8 della Direttiva riguardante i trattamenti di categorie particolari di dati.

Altro riferimento fondamentale è la Direttiva 96/9/CE "Protezione giuridica delle banche dati", definite come una raccolta di dati aventi valore economico, disposti sistematicamente ed accessibili individualmente grazie a mezzi elettronici o in altro modo. L'insieme di tali beni, in quanto dotato di determinate caratteristiche e frutto dell'ingegno del suo autore, gode di una privativa, data dal diritto d'autore, o simil-privativa, che vieta l'estrazione o il reimpiego sleale della totalità o di una parte sostanziale del contenuto della banca dati. Gli Stati membri possono comunque, come prevede l'articolo 9, stabilire che all'utente legittimo di una banca dati questa sia messa a disposizione, senza autorizzazione di chi l'ha costituita, qualora si tratti di un'estrazione per fini privati, didattici, di ricerca scientifica o di sicurezza pubblica. Tale diritto, individuato nella sua effettiva portata e qualificato nella Direttiva comunitaria come "diritto sui generis"[8], si applica alle banche dati i cui costitutori sono cittadini di uno Stato membro o risiedono abitualmente nel territorio della Comunità. Sono ovviamente gli stessi Stati membri a prevedere adeguate sanzioni contro la violazione dei diritti contemplati dalla presente Direttiva. La persona fisica o il gruppo di persone che hanno creato la banca dati godono del diritto esclusivo di autorizzare la riproduzione, traduzione e distribuzione al pubblico della banca dati, oltre alla sua comunicazione, presentazione o distribuzione in pubblico.
La Direttiva 96/9/CE, pur avendo una portata più circoscritta della Direttiva 95/46/CE, resta nell'ottica economica di tutela dei diritti di proprietà intellettuale, riferendosi sia al dato in sé e per sé, sia alla banca creata con originalità sulla base di quegli stessi dati, di natura economica e morale. In un mercato in cui l'informazione è considerata un bene, l'oggetto di un servizio offerto all'interessato o proveniente da quest'ultimo, che spontaneamente lo offre al titolare della banca per ottenere un profitto, è necessario capire quali sono i limiti e le funzioni di questo, oltre ai costi della creazione delle informazioni, delle banche dati, della loro elaborazione e del trasferimento. Gli interessi in gioco sono infatti molteplici, non riguardano solo gli utenti delle informazioni, ma anche gli elaboratori di banche dati, i pubblici e privati collegati al mondo dei media e alle funzioni essenziali ed accessorie dello Stato e delle Amministrazioni.

Le disposizioni della Direttiva 96/9/CE, adottata dal Parlamento Europeo e dal Consiglio dell'Unione Europea il 15 dicembre 1997, hanno precisato ed integrato la Direttiva 95/46/CE, prevedendo l'armonizzazione delle disposizioni degli Stati membri atte a garantire un livello equivalente di tutela dei diritti e delle libertà fondamentali, in particolar modo del diritto alla vita privata, con riguardo al trattamento dei dati personali nel settore delle telecomunicazioni.

[8] La presente direttiva, quindi, prevede un doppio regime di protezione a seconda che la banca dati possieda il requisito dell'originalità o meno. Nel primo caso la banca sarà protetta dal diritto patrimoniale d'autore nella sua formulazione classica, quindi avente durata di 70 anni, mentre nella seconda ipotesi si avrà una protezione mediante un diritto *sui generis*, volto a proteggere il contenuto della stessa dall'abusiva estrazione o reimpiego dei dati, ed avente durata limitata nel tempo di 15 anni.

3. Il mutato scenario ed il contesto GDPR

La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale dell'Unione europea. L'articolo 8, della Carta dei diritti fondamentali dell'Unione europea e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea (TFUE) stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. Il progresso tecnologico ed il mutato scenario in cui i dati sono trattati rispetto a quando era stata approvata la Direttiva 95/46/CE, nonché le divergenze del recepimento della Direttiva da parte dei vari Stati dell' Unione europea hanno reso necessaria una riforma radicale del quadro normativo europeo in materia di protezione dei dati personali al fine di dotare i vari Paesi europei di un unico *corpus* di norme tali da garantire una reale tutela del diritto delle persone alla protezione dei propri dati personali.

La Commissione europea ha promosso tale riforma, dopo aver avviato delle consultazioni pubbliche a decorrere dal 2009 e proponeva in data 25 gennaio 2012, con una comunicazione al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni rubricata "Salvaguardare la privacy in un mondo interconnesso- Un quadro europeo della protezione dei dati per il XXI secolo" un nuovo "quadro normativo solido e coerente, trasversale a tutte le politiche dell' Unione" composta da:

- Un Regolamento in sostituzione della Direttiva 95/46/CE per l'istituzione di un quadro europeo generale in materia di protezione dati personali
- Una Direttiva in sostituzione della decisione quadro 2008/977/GA116 per stabilire le norme applicabili alla protezione dei dati personali trattati ai fini di prevenzione, indagine, accertamento o perseguimento dei reati e relativa attività giudiziaria.

Il progetto di regolamento veniva adottato dal Parlamento europeo il 14 aprile 2016, in data 4 maggio 2016 la riforma si concretizzava con la pubblicazione in Gazzetta Ufficiale dell'Unione europea(L119):

- del Regolamento europeo 2016/679 del 27 aprile 2016 del Parlamento europeo e del Consiglio" relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE (regolamento generale sulla protezione dei dati)
- della Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, "relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di

reati o esecuzione di sanzioni penali, nonché della libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio".

Un *corpus* unico di norme in tutti i Paesi europei, a beneficio dei cittadini, ma anche delle imprese e delle pubbliche amministrazioni con la semplificazione di alcuni adempimenti ed una elevata responsabilizzazione.

Il Regolamento europeo 679/2016 è diventato definitivamente applicabile in via diretta in tutti i Paesi dell'Unione europea a decorrere dal 25 maggio 2018. Con tale Regolamento la normativa in materia di protezione dei dati personali ha assunto un ruolo centrale e determinante per l'adozione di qualsiasi decisione che implichi un trattamento di dati personali da parte di soggetti (imprese, liberi professionisti, ecc.) anche stabiliti in Paesi non appartenenti all' Unione europea, ivi incluse le pubbliche amministrazioni. Il Regolamento attribuisce alla Commissione europea il potere di adottare atti delegati e di esecuzione e consente ai singoli Stati membri dei margini di manovra per precisare alcune norme e le condizioni alle quali il trattamento è lecito, così come interventi specifici da parte delle Autorità di controllo. A livello europeo, le Autorità di protezione dei dai personali dei singoli Stati membri hanno operato congiuntamente, nell' Ambito del Gruppo di Lavoro Articolo 29 (sostituito dal Comitato europeo per la protezione dei dati dotato di maggiori poteri) per l'adozione di linee guida e strumenti volti a facilitare l'applicazione del nuovo quadro giuridico. Il Comitato europeo ha provveduto ad approvare tutti i documenti predisposti dal Gruppo di lavoro Articolo 29 nel corso del 2017 e 2018 nonché ad adottarne di nuovi tra cui: Linea Guida sul Consenso ai sensi del Regolamento (UE) 2016/ 679 e Linea Guida sulla trasparenza ai sensi del Regolamento (UE) 2016/ 679.

A livello nazionale, l'art.13 della legge di delegazione europea 25 ottobre 2017, n. 163 aveva delegato il Governo ad adottare uno o più decreti legislativi al fine di adeguare il quadro normativo nazionale alle disposizioni del Regolamento (UE) 2016/679, stabilendo l'osservanza, oltre che dei principi e criteri direttivi generali, anche dei seguenti principi e criteri direttivi specifici:

a) abrogare le disposizioni del codice in materia di trattamento dei dati personali, di cui al decreto 196/2003, incompatibili con le disposizioni del Regolamento (UE) 2016/679:
b) modificare il codice di cui al decreto legislativo 30 giugno 2003, n. 196, limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili contenute nel Regolamento (UE) 2016/679;
c) coordinare le disposizioni vigenti in materia di trattamento dei dati personali con le disposizioni del Regolamento (UE) 2016/679

d) prevedere, ove opportuno, il ricorso, a specifici provvedimenti attuativi ed integrativi adottati dal Garante per la protezione dei dati personali nell'ambito e per le finalità previsti dal Regolamento (UE) 2016/ 679;
e) adeguare, nell'ambito delle modifiche al codice di cui al decreto legislativo 196/2003, il sistema sanzionatorio.

In attuazione dell'art.13 della L. 163/2017, il legislatore nazionale ha adottato il decreto legislativo 10 agosto 2018, n.101 che ha:

- abrogato molteplici disposizioni del decreto legislativo 30 giugno 2003, n, 196 incompatibili con il Regolamento;
- modificato altre disposizioni del decreto legislativo 30 giugno 2003, n. 196, ove necessario;
- introdotto nuove disposizioni all' interno del decreto legislativo 30 giugno 2003, n. 196;
- previsto una serie di disposizioni di carattere transitorio

Come precisato anche dal D. Lgs 101/2018 con una clausola interpretativa a valenza generale, le disposizioni nazionali devono, comunque, essere interpretate ed applicate alla luce della disciplina dell'Unione europea in materia di protezione dei dati personali.
Si tratta di canone interpretativo desumibile anche dalla gerarchia delle fonti del diritto e dall' art. 288 del Trattato sul funzionamento dell'Unione europea (TFUE) che stabilisce la portata del Regolamento, obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

Nella gerarchia delle fonti i Regolamenti si collocano prima delle leggi statali ancorché successive nel tempo e prevalgono sulla legislazione interna.

3.1. Le novità del Regolamento europeo 2016/ 679

Il Regolamento europeo 2016/679 nel confermare concetti noti nell' ordinamento italiano, introduce novità di carattere sostanziale al fine di garantire un elevato livello di tutela degli interessati basato sull' analisi dei rischi e sulla responsabilizzazione (accountability) dei soggetti che trattano i dati, anche se non stabiliti nell' Unione europea, nel caso trattino dati di interessati che si trovano nell' Unione. Ai singoli Stati membri sono consentiti margini di manovra per precisare alcune norme e le condizioni alle quali il trattamento è lecito. Il legislatore italiano è intervenuto apportando modifiche sostanziali al D. Lgs 196/2003 ("Codice Privacy") con l'adozione del D. Lgs. 101/2018.

Di seguito si riepilogano le principali novità introdotte dal Regolamento e dal D. Lgs 196/2003, come novellato dal D. Lgs 101/2018:

- Il nuovo principio di responsabilizzazione (*accountability*) rappresenta il punto centrale della normativa in materia di protezione dei dati personali. Secondo tale principio, il Titolare è obbligato a mettere in atto "misure tecniche ed organizzative adeguate" che devono essere costantemente monitorate ed aggiornate, se necessario, "per garantire, ed essere in grado di dimostrare" che il trattamento è effettuato conformemente al Regolamento.
- Il Titolare deve mettere in atto delle misure tecniche ed organizzative per attuare i principi di protezione dei dati fin dalla progettazione (*Privacy by design*) e per impostazione predefinita (*Privacy by default*)
- I diritti degli interessati risultano ampliati, il Regolamento include il nuovo "diritto alla portabilità dei dati" ed il diritto all' oblio
- Viene introdotta la figura del Responsabile della protezione dei Dati (*Data Protection Officer*), da non confondere con il responsabile del trattamento dati. Tale figura deve essere obbligatoriamente designata in caso di trattamento effettuato da un'Autorità pubblica o un organismo pubblico, o se il Titolare o il Responsabile effettuano un trattamento che richiede un monitoraggio su larga scala, oppure se vengono effettuati trattamenti su larga scala di categorie particolari di dati o dati relativi a condanne penali o reati.
- Viene introdotto per il Titolare ed il Responsabile del trattamento il nuovo obbligo di tenere un registro delle attività di trattamento in forma scritta, anche in formato elettronico.
- Le persone che trattano dati personali devono essere debitamente autorizzate ed istruite, potendo anche attribuire specifici compiti e funzioni a persone espressamente designate ai sensi del nuovo art 2 *quaterdecies* del dlgs 196/2003.
- L'informativa deve essere coincisa, trasparente, intellegibile, facilmente accessibile, deve essere resa con un linguaggio semplice e chiaro soprattutto in caso di trattamento di dati di minori.
- È necessario valutare il rischio per i diritti e le libertà degli interessati relativo alle operazioni di trattamento in termini di gravità e probabilità e di individuare le situazioni in cui il rischio dovesse essere elevato per porre in atto le azioni richieste dal Regolamento.
- È obbligatorio effettuare una valutazione di impatto sulla protezione dei dati e consultare preventivamente l'autorità di controllo se la valutazione di impatto evidenzia un rischio elevato in assenza di misure per attenuare il rischio.
- Qualsiasi violazione di dati personali (c.d. *data breach*) deve essere notificata al garante entro il termine di 72 ore e, in presenza di determinati presupposti, anche agli interessati. Viene eliminato l'obbligo di notificazione preventiva.
- Viene introdotta l'adozione di codici di condotta e di meccanismi di certificazione.

- Sono attribuiti maggiori poteri alle autorità di controllo nazionali, definiti i compiti e i poteri dell'autorità di controllo capofila.
- L'impianto sanzionatorio diventa particolarmente severo con sanzioni amministrative, penali e civili. Le sanzioni amministrative pecuniarie, che devono essere effettive, proporzionate e dissuasive in relazione al singolo caso, possono arrivare fino a euro 20 milioni o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore. Le sanzioni penali come modificate ed innovate nel D. Lgs 196/2003 come novellato prevedono la reclusione fino a sei anni. Chiunque, inoltre può promuovere un'azione per risarcimento dei danni materiali ed immateriali conseguenti ad un illecito trattamento di dati personali.

3.2. L'ambito di applicazione del Regolamento ed i concetti essenziali

Il Regolamento UE 2016/679 si applica a qualsiasi trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi, intendendosi per "archivio" "qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico".

Per espressa previsione dell'art. 2, par.2, il Regolamento non si applica al trattamento di dati personali:

- Effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione;
- Effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE;
- Effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale e domestico;
- Effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali.

Restano esclusi inoltre dall'ambito di applicazione del Regolamento i dati anonimi, o i dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato. Il trattamento di dati personali da parte di istituzioni, organi, uffici ed agenzie dell'Unione europea è invece soggetto alle disposizioni del Regolamento (CE) n.45/2001.

Ai sensi dell'art.3, il Regolamento si applica ai Titolari ed ai Responsabili del trattamento stabiliti in uno Stato dell'Unione Europea. Il Considerando 22 precisa come lo "stabilimento" implichi l'effettivo e reale svolgimento di attività nel quadro di un'organizzazione stabile, senza che abbia alcuna rilevanza la forma giuridica assunta. Il Regolamento UE 2016/679 si applica, inoltre, ai Titolari o Responsabili non stabiliti nell'Unione europea se trattano i dati personali di interessati che si trovano nell'Unione europea, quando le attività di trattamento riguardano:

1) L'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione;
2) Il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.

Il Regolamento si applica al trattamento dei dati personali di una persona fisica. Concetti fondamentali quali il dato personale ed il trattamento, nonché delle definizioni di ogni termine contenute nell'art.4 del Regolamento, risultano essenziale per la corretta applicazione del Regolamento UE 2016/679.

L'art.4 par.1, del Regolamento definisce il dato personale come qualsiasi informazione riguardante una persona fisica identificata e identificabile, ivi inclusi i dati personali sottoposti a tecniche di pseudoanonimizzazione. Sono considerati a titolo meramente esemplificativo "dati personali" il nome ed il cognome di un individuo, il numero di telefono o di cellullare, l'indirizzo e-mail, il codice fiscale, l'immagine fotografica di una persona, una registrazione vocale, una targa automobilistica ecc. Nell'ambito dei dati personali il Regolamento individua le seguenti tipologie di dati personali il cui trattamento merita una specifica protezione ed è consentito solo in presenza di determinate condizioni:

- Le categorie particolari di dati personali;
- I dati personali relativi a condanne penali e reati;
- Dati dei minori.

L'art.9 del Regolamento identifica come "categorie particolari di dati personali":

- I dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale;
- I dati genetici[9];

[9] L'art. 4, punto 13, del Regolamento definisce i "*dati genetici*" come i "dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione".

- I dati biometrici[10] intesi a identificare in modo univoco una persona fisica;
- I dati relativi alla salute[11] o alla vita sessuale o all'orientamento sessuale della persona.

Il Regolamento prevede per il trattamento di tali categorie di dati personali una tutela rafforzata. L'art.10 del Regolamento prevede una tutela rafforzata anche nel caso di trattamento dei dati relativi a condanne penali o reati, consentito solo sotto il controllo dell'autorità pubblica, ovvero se autorizzato dal diritto del Unione europea o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Il Regolamento richiede una tutela rafforzata anche nel caso di trattamento dei dati personali del minore sia per quanto concerne le modalità con cui fornire le informazioni sul trattamento dei dati personali come richiesto dall'art.12 del Regolamento, sia con riferimento all'espressione del relativo consenso nell'ambito dei servizi della società dell'informazione come previsto dall'art.8 del Regolamento. Il Regolamento prevede sedici anni quale soglia minima per l'espressione di un valido consenso, consentendo agli Stati membri di stabilire un'età inferiore purché non al di sotto dei tredici anni.

L' art.9 del Regolamento identifica come "categorie di dati particolari di dati personali":

- I dati personali che rivelino l'origine razziale o entica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale;
- I dati genetici;
- I dati biometrici intesi a identificare in modo univoco una persona fisica;
- I dati relativi alla salute o alla vita sessuale o all' orientamento sessuale della persona.

  Per tali categorie di dati personali il Regolamento prevede una tutela rafforzata, come previsto dalla normativa nazionale, modificata ad opera del D. Lgs. 101/2018 che ha introdotto nel D. Lgs. 196/2003 l'art.2-sexies che disciplina il trattamento delle categorie particolari di dati personali necessario per motivi di interesse pubblico, e l'art.2-septies, che detta le misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute.

Il **dato pseudo-anonimizzato** è un dato personale sottoposto a delle misure atte a non consentire l'attribuzione di tale dato personale ad un interessato specifico senza l'utilizzo di informazioni aggiuntive che sono conservate separatamente e soggette a misure tecniche ed organizzative. La pseudo- anonimizzazione è una misura tecnica adeguata. Non si tratta di una misura di

[10] L'art. 4, punto 14, del Regolamento definisce i "*dati biometrici*" i "dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali immagine facciale o i dati dattiloscopici".

[11] L'art. 4, punto 15, del Regolamento definisce i "*dati relativi alla salute*" 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". Il considerando 35 del Regolamento chiarisce 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" e precisa ulteriormente che tali dati "comprendono informazioni sulla persona fisica raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria o della relativa prestazione".

anonimizzazione, bensì di una modalità per "ridurre la correlabilità di un insieme di dati all'identità originaria di una persona interessata, e rappresenta pertanto una misura di sicurezza utile".

Il **dato profilato** è un dato sottoposto a tecniche di profilazione intesa come "qualsiasi forma di trattamento automatizzato di dati personali consistente nell' utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l' affidabilità, il comportamento, l' ubicazione, o gli spostamenti di detta persona fisica".

Il **trattamento** è inteso come "qualsiasi operazione o insieme di operazioni" tra quelle elencate nell' art. 4, punto 2 del Regolamento, dalla raccolta fino alla cancellazione o distruzione del dato.
I concetti di dato personale e di trattamento sono, pertanto, molto ampi e tali da comprendere qualsiasi informazione e l'intero ciclo di vita di un dato personale.

3.3. I principi e le figure soggettive

I nuovi principi di trasparenza e responsabilizzazione ("accountability") sono l'elemento di novità rispetto ai già noti principi presenti nell' ordinamento italiano quali liceità, correttezza, finalità, adeguatezza, pertinenza, esattezza, minimizzazione, limitazione della conservazione.
Di seguito quanto disposto dall' art.5 del Regolamento, i dati personali devono essere:

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato ("liceità, correttezza e trasparenza");
- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità ("limitazione della finalità");
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati ("minimizzazione dei dati");
- esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono stati trattati ("esattezza");
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati ("limitazione della conservazione");

- trattati in modo da garantire un'adeguata sicurezza dei dati personali, compresa la protezione mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale ("integrità e riservatezza").

Il Titolare deve rispettare i predetti principi e deve essere in grado di comprovarlo ("responsabilizzazione"). Il principio di liceità è normato dall' art.6 del Regolamento, il trattamento è lecito solo se ricorre almeno una delle seguenti condizioni:
a) l'interessato ha espresso il consenso al trattamento dei proprio dati personali per una o più specifiche finalità;
b) il trattamento è necessario all' esecuzione di un contratto di cui l'interessato è parte o all' esecuzione di misure precontrattuali adottate su richiesta dello stesso;
c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il Titolare del trattamento;
d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato di un'altra persona fisica;
e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all' esercizio di pubblici poteri di cui è investito il Titolare del trattamento;
f) con esclusione del trattamento di dati effettuato dalle autorità pubbliche nell' esecuzione dei loro compiti, il trattamento è necessario per il perseguimento del legittimo interesse del Titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

Il principio di liceità identifica le basi giuridiche per il trattamento dei dati come elencate nel suddetto art.6, mentre il trattamento dei dati appartenenti a categorie particolari e dei dati relativi a condanne penali e reati richiede anche l'osservanza delle condizioni previste, rispettivamente dagli artt. 9 e 10 del Regolamento.

Il principio di trasparenza si sostanzia nell' obbligo del Titolare del trattamento di informare gli interessati in merito al trattamento dei loro dati personali, di rendere le informazioni richieste in caso di esercizio dei diritti e di informare gli interessati in caso di violazione di dati personali.

Il principio di responsabilizzazione o accountability consiste nell' obbligo del Titolare di dimostrare il rispetto dei principi di trattamento dei dati e di mettere in atto "misure tecniche ed organizzative adeguate" che devono essere esaminate ed aggiornate, se necessario, "per garantire ed essere in grado di dimostrare" che il trattamento è conforme al Regolamento.

Il Regolamento identifica specifici soggetti e specifici ruoli, alcuni dei quali già noti e disciplinati dal D. Lgs 196/2003, ed introduce la nuova figura del Responsabile del Protezione dei Dati, anche noto con la terminologia anglosassone di *Data Protection Officer* (DPO), non esistente nella previgente legislazione nazionale italiana. L' interessato è il soggetto persona fisica (identificato o identificabile) i cui dati personali sono oggetto di trattamento i cui diritti e libertà fondamentali sono tutelati dal Regolamento.

Il Titolare del trattamento è "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri". Il Titolare è il soggetto su cui grava la responsabilità generale del trattamento, che deve adempiere alle prescrizioni contenute nelle varie disposizioni del Regolamento e deve mettere in atto misure tecniche ed organizzative adeguate a essere in grado di dimostrare che il trattamento dei dati personali è effettuato conformemente al Regolamento secondo il principio di responsabilità, ivi inclusa l'efficacia delle misure adottate. Viene introdotta un'elevata responsabilizzazione del Titolare che deve avere un approccio proattivo valutando costantemente il contesto ed il settore in cui opera per poter garantire la conformità delle operazioni di trattamento dei dati personali. Gli artt.24 e 25 del Regolamento individuano gli obblighi generali in capo al Titolare ed il Titolare può dimostrare il rispetto degli obblighi a suo carico anche attraverso l'adesione a codici di condotta o a meccanismi di certificazione di cui agli artt. 40-43 del Regolamento.

3.4. Adeguamento della normativa nazionale alla legislazione europea

La nuova regolazione della protezione dati, non era destinata a rimanere prerogativa esclusiva del legislatore europeo, poiché, pur rappresentando il GDPR la normativa fondamentale di riferimento in materia, esso stessa rinvia, per la sua attuazione ed integrazione, alle legislazioni nazionali, che in tutti gli Stati membri necessitavano di un intervento riformatore di adeguamento al mutato contesto sovranazionale. Così è stato anche per il nostro Codice della privacy, approvato con decreto legislativo 30 giugno 2003, n.196, che è stato oggetto di una profonda revisione con il decreto legislativo 10 agosto 2018, n. 101, che, pur assumendo formalmente la veste di una novella del testo precedente, ne ha abrogato gran parte delle disposizioni e ne ha modificato quelle residue al fine di tener conto delle nuove regole europee.

La disciplina privacy in Italia, come noto, è stata oggetto di una regolazione organica soltanto da poco più di vent'anni. Nonostante l'introduzione di un tale corpus normativo sia dunque piuttosto recente, si sono succeduti già ben tre interventi codificatori. L'instabilità di questa normativa non stupisce, è infatti ben noto che il diritto in questione ha fin dalla sua origine uno stretto legame con l'evoluzione tecnologica, la quale pur comportando l'emergere di nuovi rischi, ne ha sempre segnato ed accompagnato lo sviluppo.

Il Regolamento UE n. 679/2016, lungi dal disciplinare in modo esaustivo la materia, rinvia esplicitamente in più parti al diritto dei singoli stati membri. Gli Stati membri, di conseguenza, hanno provveduto a adeguare le loro legislazioni nazionali in modo che le stesse, concepite in periodi storici, ed in contesti tecnologici diversi, potessero presentarsi in sintonia con lo spirito della nuova normativa europea. Del resto, la dilazione di due anni tra l'entrata in vigore del GDPR e la sua effettiva applicabilità trovava giustificazione anche nella necessità di lasciare un tempo sufficiente agli Stati membri proprio affinchè, attraverso l'adeguamento delle legislazioni nazionali, dal 25 maggio 2018 queste potessero formare un corpus coerente con la disciplina europea.

Il legislatore italiano non si è sottratto a questo compito e, opportunamente, con la legge di delegazione europea del 2017 (L. 25 ottobre 2017 n. 163) ha avviato il procedimento per l'adeguamento dell'ordinamento interno in previsione della effettiva applicabilità del Regolamento. In particolare, l'art 13 di tale atto normativo delegava il Governo all'adozione di uno o più decreti legislativi per l'adeguamento dell'ordinamento interno al GDPR. Nello specifico, tale revisione, aveva anzitutto l'obiettivo di provvedere all'abrogazione espressa delle disposizioni del Codice incompatibili con il nuovo Regolamento UE. In secondo luogo, al legislatore delegato veniva affidato il compito di modificare le norme del Codice al mero fine di attuare le disposizioni del GDPR non direttamente applicabili nonché di coordinare le norme residue con la normativa europea, in modo tale da far sì che ne risultasse un corpus normativo sistematico e coerente. Da ultimo, la legge delega, per un verso, prevedeva la facoltà di delegificare alcuni ambiti della materia, attribuendo a provvedimenti generali dell'Autorità Garante la regolazione di essi, sia per una finalità puramente attuativa che anche integrativa, nei limiti della discrezionalità lasciata agli Stati membri da parte del Regolamento, mentre per altro verso, affidava al Governo il compito di intervenire in modo specifico sull'apparato sanzionatorio amministrativo e penale. Alla luce di questa delega legislativa e dei criteri poc'anzi richiamati, il 14 dicembre 2017 il Governo nominava una commissione di esperti, presieduta da Giusella Finocchiaro, per la redazione del testo del decreto delegato, la quale concludeva i propri lavori alla metà di marzo dell'anno successivo. Il 21 marzo 2018 il Governo adottava, con delibera preliminare, lo schema di decreto, che poi veniva trasmesso, secondo le previsioni della medesima legge delega, sia al Garante per la protezione dei dati personali che alle commissioni parlamentari al

fine dell'espressione del parere. Il testo definitivo del decreto legislativo in commento è stato emanato dal Capo di Stato il 10 agosto del 2018.

L'impatto più significativo che il dlgs. n.101/2018 ha avuto sulla disciplina previgente è certamente quello sul Codice che esso va a novellare (Dlgs.196/2003), un dato assai rilevante è difatti l'abrogazione espressa di 109 disposizioni codicistiche (che si aggiungono alle 4 già eliminate con l'approvazione del d.lgs. n.51/2018). Tale abrogazione è solo in parte compensata dall'aggiunta di 26 articoli, di modo che ciò che resta del Codice è ormai un testo normativo con ampi vuoti tra un gruppo e l'altro di disposizioni residue. Alla luce di queste significative modifiche operate sul testo del Codice, l'art 22 del decreto legislativo in commento contiene una nutrita serie di disposizioni finali e di coordinamento: Anzitutto va ricordata la norma di cui al primo comma dell'articolo in questione, che prescrive l'adozione di un'interpretazione delle disposizioni del decreto e in generale di diritto interno in subiecta materia in senso conforme al GDPR. Lo stesso art. 22 regola poi i riferimenti normativi al Codice previsti nella legislazione vigente, affermando in generale che laddove le norme richiamate siano state abrogate il rinvio vada riferito alle corrispondenti norme del GDPR ed a quelle del Codice, come modificato. Una norma specifica è poi prevista per i trattamenti svolti per l'esecuzione di un compito pubblico che comportino un rischio elevato, i quali possono proseguire, nelle more dei provvedimenti generali del Garante previsti dal nuovo art.2-quinquiesdecies, se disciplinati con legge, regolamento o atto amministrativo generale ovvero se hanno costituito oggetto di verifica o autorizzazione da parte del Garante stesso. A conferma del mutato quadro legislativo lo svolgimento di compiti di interesse pubblico può essere una base giuridica che giustifica il trattamento da parte del titolare a prescindere dalla natura (pubblica o privata) di questi.

Attenzione particolare merita l'incidenza del "nuovo" Codice sui commi 1022 e 1023 dell'unico articolo della legge di bilancio per il 2018, che con un intervento estemporaneo era intervenuta sul tema della protezione dei dati. I due commi in questione prevedono in particolare, che il titolare, che voglia effettuare trattamenti con mezzi automatizzati o nuove tecnologie, debba comunicarlo preventivamente al Garante, trasmettendo a questi un'informativa indicante alcuni elementi previsti dalla legge. L'Autorità, nel caso di accertato rischio per le libertà e i diritti degli interessati, può disporre una moratoria del trattamento per un termine di 30 giorni al fine di acquisire ulteriori elementi, potendo poi inibirlo in toto nel caso di persistenza del rischio. Viceversa, in caso di mancata risposta, il titolare può iniziare il trattamento trascorsi 15 giorni dalla notifica. Si tratta dell'introduzione di una vera e propria autorizzazione, con il meccanismo del silenzio assenso. In ogni caso il d.lgs. n.101/2018 ha poi circoscritto l'applicabilità di queste previsioni ad un unico caso, ovvero i trattamenti funzionali all'autorizzazione al cambiamento del nome e del cognome dei minorenni. Se poi si considera che la Pubblica Amministrazione non può, per espressa previsione del

Regolamento, ricorrere al legittimo interesse come base giuridica per i propri trattamenti, si rende evidente come i due commi in questione siano destinati a trovare un'applicazione alquanto sporadica.

Rilevante è sicuramente l'impatto del "nuovo" Codice rispetto alle autorizzazioni generali del Garante, ossia provvedimenti *erga omnes* che, nella vigenza del testo precedente, potevano essere adottati, ogniqualvolta fossero previste specifiche autorizzazioni, per categorie di titolari o di trattamenti con la pubblicazione in Gazzetta Ufficiale e che non sono invece più previsti dal Regolamento. Con riferimento a tali provvedimenti è affidato al Garante stesso il compito di individuare quali di essi sia incompatibili con il GDPR e quali invece possano considerarsi tuttora validi e meritevoli di conservare efficacia. La previsione peraltro non riguarda tutte le autorizzazioni, bensì soltanto quelle concernenti i trattamenti che trovano la loro base giuridica nell'adempimento di un obbligo legale o nello svolgimento di un compito di pubblico interesse (art. 6, par.1, lett. c) ed e) del GDPR), quelli relativi a dati particolari trattati in adempimento di obblighi in ambito giuslavoristico o comunque riferiti a dati relativi alla salute, genetici o biometrici. Appare insomma evidente la preoccupazione del legislatore di non creare vuoti normativi, che avrebbero comportato l'estrema difficoltà, se non l'impossibilità di proseguire, a causa della mancanza di idonee garanzie, trattamenti in ambiti che si rilevano invece imprescindibili. L'art.21.4 stabilisce poi per i trattamenti fondati sull'adempimento di un obbligo legale o sulla salvaguardia degli interessi vitali dell'interessato ovvero per quelli concernenti i dati relativi alla salute, biometrici e genetici, l'adozione rispettivamente di regole deontologiche e di misure di garanzia.

Alla luce di quanto visto, sembra piuttosto evidente come la forte incidenza del d.lgs. n. 101/2018 sull'ordinamento possa portare a discorrere di un Codice sostanzialmente nuovo, pur sotto la veste formale di un mero restyling del precedente. Si pone l'interrogativo, se si riveli davvero opportuna la scelta del legislatore interno di mantenere l'involucro del testo normativo vigente anziché abrogarlo sostituendolo con un testo diverso, magari abbandonando lo stesso nomen di Codice. La scelta effettuata dal Governo merita di essere condivisa. Infatti, il testo normativo attualmente in vigore presuppone il Regolamento UE tanto da porsi rispetto ad esso come un testo in autonomo, ossia presuppone un coordinamento con il GDPR come del resto dichiara espressamente l'art.2 del Codice stesso. Il testo non sarebbe solo privo di autonomia, ma risulterebbe quasi incomprensibile e privo di senso se non letto con il GDPR. Ciò, tuttavia, non far venire meno la considerazione che quell'atto normativo è pur sempre un codice, inteso come testo che racchiude, cercando di darvi una sistemazione per quanto organica, la legislazione nazionale vigente in materia ed ogni altra disposizione attuativa del GDPR. Il Codice non esaurisce la materia, gran parte di essa è sottratta alla regolazione nazionale, ciò tuttavia non fa venir meno l'opportunità di continuare a raccogliere tutta questa in un solo atto, in modo che alla armonizzazione con la normativa europea si accompagni la

razionalizzazione di quella interna. Il Codice non risulta perciò esaustivo per l'ampio ricorso che viene fatto ai provvedimenti generali del Garante o a regole deontologiche e codici di condotta, che solo in parte sono destinati ad entrare nell'atto normativo de quo, peraltro come meri allegati.

Nella sostanza emerge, da questo assetto delle fonti, che si apre una nuova stagione nella protezione dei dati personali, in cui la regolazione unitaria a livello europeo assume un valore decisivo, laddove l'intervento del legislatore interno è destinato ad essere, se non marginale, quanto meno integrativo e complementare rispetto a quello sovranazionale. Ciò è tanto più vero per il fatto che esso sarà tenuto ad ispirarsi, nel solco dell'impostazione del GDPR, ad una regolazione leggera, che conservi ampio margine alla responsabilizzazione del singolo titolare, fin dalla fase di progettazione del trattamento, quale principio cardine dell'intero quadro normativo. La centralità del principio di *accountability*, che si sostanzia alla valorizzazione dell'assunzione di responsabilità da parte dei singoli titolari in particolare nella valutazione del livello di rischio dei trattamenti e della conseguente necessità di adottare gli adempimenti previsti normativi nonché dell'adeguatezza delle misure di protezione, segna un profondo cambiamento culturale e una netta censura rispetto all'imposizione della normativa precedente. Si è passati ad una prima regolazione fondata sulla visione proprietaria dei dati, in cui le autorizzazioni e in più generale i controlli preventivi del Garante rivestivano un peso rilevante, fino ad una legislazione che ha progressivamente lasciato all'Autorità pubblica un ruolo di mero soggetto regolatore, a fronte di una valorizzazione, sotto il profilo sostanziale, dell'assunzione di responsabilità del singolo titolare del trattamento, laddove l'intervento del Garante è pensato in ottica non burocratica e autorizzatoria ma di controllo e di eventuale sanzione a posteriori nel caso in cui si sia verificato un abuso del margine di autovalutazione lasciato ai singoli. La privacy si conferma, così, come un diritto dal carattere fortemente dinamico che richiede un adattamento al mutare delle esigenze della società e della tecnologia ancor più repentino di altre situazioni soggettive. Quindi il d.lgs. n. 101/2018 non rappresenta che uno dei tanti passaggi, nell'attesa dei prossimi ed inevitabili interventi legislativi volti tanto a migliorare la omogeneità del sistema e la qualità complessiva della legislazione in materia quanto ad inseguire l'evoluzione continua del diritto de quo.

4. Il trattamento dei dati personali nell'ambito del rapporto di lavoro post GDPR

L' entrata in vigore del Regolamento Generale sulla Protezione dei Dati ha reso necessario l'adeguamento della disciplina interna alle nuove norme concernenti la protezione dei dati personali. Con riferimento ai rapporti di lavoro, il progredire delle tecnologie informatiche ha acuito l'esigenza di bilanciare, da un lato il legittimo interesse del datore di lavoro alla salvaguardia del patrimonio e

dell'organizzazione aziendale, dall' altro "gli interessi o i diritti e le libertà fondamentali"[12] del lavoratore impegnato nell' attività lavorativa. Rispetto al passato, lo scenario di riferimento è cambiato; l'introduzione di Internet sugli strumenti di lavoro, il diffuso utilizzo dei servizi elettronici di posta nei rapporti lavorativi ha incentivato l'uso delle tecnologie colpendo "la tradizionale separazione tra apparecchiature di controllo e strumenti di lavoro, oltre che, più in generale, tra momenti di vita e lavoro"[13]. Inoltre, la diffusione di forme di lavoro "agili", all' interno di questo "ecosistema digitale"[14] sempre più (inter)connesso ha reso il "controllo dell'informazione una componente essenziale del rapporto di lavoro, e ciò a prescindere dalla sua qualificazione giuridica"[15]. Per quanto concerne il trattamento dei dati personali nell'ambito dei rapporti lavorativi il GDPR ha attribuito agli stati membri la potestà di prevedere norme più specifiche per il tramite di leggi o contratti collettivi[16], al fine di assicurare la protezione dei diritti e delle libertà che ineriscono la gestione dei dati personali dei dipendenti.

L'articolo 88 primo comma del GDPR, ha precisato che la suddetta facoltà è conferita "per finalità di assunzione, esecuzione del contratto di lavoro, […] di gestione pianificazione ed organizzazione del lavoro" così come in materia di parità di trattamento, salute e sicurezza sul lavoro. Inoltre, il secondo comma dell'articolo 88 prosegue imponendo la predisposizione di "misure appropriate e specifiche a salvaguardia della dignità umana, degli interessi legittimi e dei diritti fondamentali degli interessati, in particolare per quanto riguarda la trasparenza del trattamento, il trasferimento di dati personali nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune e i sistemi di monitoraggi sul posto di lavoro".

Il legislatore italiano ha provveduto ad adeguare le disposizioni contenute nel Codice della Privacy alle indicazioni racchiuse nel nuovo dettato normativo europeo. Il novellato D. Lgs 196 2003 detta la disciplina in materia di rapporto di lavoro negli articoli da 111 a 116 confermando la disciplina previgente ed apportando degli aggiornamenti normativi. Le novità sono introdotte dall'articolo 9, d.lgs. 10/08/2018 n. 101. Anzitutto, in relazione al trattamento dei dati personali effettuato nell'ambito del rapporto di lavoro per le finalità di cui all'articolo 88 del Regolamento, l'articolo 111 prevede che il Garante promuova, ai sensi dell'art. *2-quater*, l'adozione di regole deontologiche dei

[12] Cfr. articolo 6, comma 1, lett. f) GDPR
[13] CARTA C., *I limiti al potere di controllo sui lavoratori nell'uso di internet e dei servizi di comunicazione elettronica: per un diritto alla moderazione*, in *Labor*, 2018, 2, p. 174; PIZZOFERRATO A., *Gli effetti del GDPR sulla disciplina del trattamento aziendale dei dati del lavoratore, in Argomenti Dir. Lav*., 2018, n. 4-5 p- 1037. Il rischio connesso alla violazione della riservatezza dei lavoratori nascente dall'uso promiscuo degli strumenti di lavoro è uno dei nove scenari tipici di rischio individuati dal Gruppo di lavoro *ex* articolo 29 ("WP29"), così denominato in quanto previsto dall'articolo 29 della direttiva 95/46/CE. L' *European Data Protection Board*, o comitato europeo per la protezione dei dati è l'organismo che ha sostituito il WP29 in seguito all'applicazione del GDPR.
[14] L'espressione è di PIZZOFERRATO A., *Gli effetti*, cit., p. 1035
[15] COSTANTINI F., *Il Regolamento (UE) 679/2016 sulla protezione dei dati personali*, in *Lav. Giur*., 2018, p.553.
[16] Cfr. articolo 88, comma 1, GDPR.

soggetti pubblici e privati prevedendo anche specifiche modalità per le informazioni da rendere all'interessato.

È previsto inoltre che:

- Nei casi di ricezione dei curricula spontaneamente trasmessi dagli interessati al fine dell'instaurazione di un rapporto di lavoro, le informazioni all' interessato vengono fornite al momento del primo contatto utile, successivo all' invio del curriculum medesimo ed il consenso per il trattamento dei dati presenti nei curricula non è dovuto nei limiti di cui all' art.6, par.1, lett. b. L' introduzione dell'art.111-bis nel Codice della privacy, ad opera dell'art.9, comma1, lett. c, d.lgs. n. 101/2018, si riferisce alle informazioni che le aziende o le agenzie per il lavoro sono chiamate a rendere in caso di ricezione di curricula trasmessi spontaneamente da soggetti interessati ad instaurare un rapporto lavorativo. In conclusione, il legislatore ha disciplinato due distinte situazioni; la prima prevede l'obbligo per tutti i soggetti economici operanti nel mercato del lavoro di predisporre un'idonea informativa da rendere, preventivamente, ai potenziali candidati interessati ad inviare curricula in risposta alle offerte di lavoro pubblicate in quotidiani o periodici. La seconda situazione invece si realizza in caso di invio spontaneo di curricula, in queste ipotesi, il legislatore ha consentito il regolare trattamento dei dati personali ivi contenuti anche quando l'informativa sia stata comunicata successivamente, purché, in occasione del primo contatto utile. Inoltre con riferimento alla condizione richiamata dall' art.6, comma1, lett. b del GDPR, il legislatore delegato ha previsto che la mancanza del consenso espresso al trattamento dei dati, in calce al curriculum, non pregiudica il regolare trattamento delle informazioni personali quando l' invio di quest' ultimo è avvenuto: 1) allo scopo di dare esecuzione ad un contratto di cui l' interessato è parte; 2) con la finalità di dare attuazione a misure precontrattuali adottate su richiesta dello stesso titolare dei dati personali.

- Con riferimento alla raccolta dei dati dei lavoratori trovano applicazione l'art.8 della L.300/1970 (Statuto dei Lavoratori) e l' art.10 del D.Lgs276/2003.Con riferimento al contenuto dell' articolo 113, d.lgs. n. 196/2003, il legislatore ha provveduto ad inserire nel testo della norma che già rinviava all' articolo 8, legge 20 maggio 1970, n.300, il divieto, *ratione materiae,* imposto alle agenzie per il lavoro e agli altri soggetti pubblici e privati autorizzati o accreditati di procedere ad indagini sulle opinioni dei lavoratori ed a trattamenti discriminatori, così come descritto nell' art. 10, d.lgs. n. 276/2003 in materia di occupazione e mercato del lavoro. Come noto in virtù dell'articolo 8 legge n. 300/1970 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". La portata assoluta del divieto contenuto nell'articolo 8 dello Statuto dei lavoratori non permette di effettuare nessun tipo di indagine, neanche con il consenso del prestatore di lavoro[17], consentendo le sole indagini avendo ad oggetto fatti rilevanti ai fini della valutazione dell'attitudine professionale[18].

Allo stesso modo, il divieto imposto alle agenzie per il lavoro e agli altri operatori pubblici e privati autorizzati, o accreditati, di effettuare qualsivoglia indagine, di trattare i dati personali dei lavoratori o di procedere alla preselezione di questi ultimi sulla base del sesso, dell'orientamento sessuale, dello stato matrimoniale, di famiglia o di gravidanza, nonché l'età, l'handicap, la razza o l'origine etnica del lavoratore subisce l'eccezione riservata alle caratteristiche "che incidono sulle modalità di svolgimento dell'attività lavorativa o che costituiscono un requisito essenziale e determinante al fine dello svolgimento dell'attività lavorativa"[19]. La disposizione contenuta nello Statuto, così come l'articolo 10, d.lgs. n. 276/2003 non si sovrappongono alla disciplina in maniera di privacy in ambito lavorativo poiché trattasi di normative "portatrici di *rationes* differenti"[20].

- In merito al controllo a distanza, resta ferma l'applicazione dell'articolo 4 della L. 300/1970. L'utilizzo sempre più diffuso di apparecchiature all'avanguardia che nell'attuale contesto produttivo costituiscono "quasi sempre strumenti di lavoro imprescindibili per rendere la prestazione lavorativa"[21] si pensi ad esempio all'uso del computer dello smart phone o della posta elettronica, di cui ogni lavoratore oggi non può più fare a meno, espongono il prestatore al rischio di vedere compromesso il proprio interesse legittimo alla tutela della dignità personale. Infatti, senza imposizione di limiti al potenziale controllo operato dal datore per mezzo dell'utilizzo di dispositivi elettronici si comprometterebbe il bilanciamento degli interessi. Anche il diffondersi di nuove modalità di esecuzione del rapporto di lavoro

[17] BELLAVISTA A, *I poteri dell'imprenditore e la privacy del lavoratore*, in *Dir. Lav*., 2002, 3, pp.153 ss.;
ID., *Privacy e protezione dei dati personali nel rapporto di lavoro subordinato: problemi e prospettive*, in *Vita not*., 1995, 3, pp.1589 ss.;
ID., *Il controllo sui lavoratori*, *Giappichelli*, Torino, 1995.

[18] Cfr. Cass. Civ. sez. lav., 17 luglio 2018, n. 19012, in D & G. 2018, 18 luglio, secondo cui: "La richiesta del certificato penale integra un limite 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 di date informazioni relative all'esistenza di condanne penali passate in giudicato. Tale limite, in assenza di espressa previsione contrattuale, non può essere dilatato per via interpretativa fino a ricomprendere informazioni relative a procedimenti penali in corso […] ciò specie in considerazione del principio costituzionale della presunzione di innocenza". Inoltre, con riferimento alla casistica legata alla fattispecie dei test attitudinali, si veda: Pretura Pisa, 30 marzo 1999, in D & L, 1999, p. 519; la giurisprudenza ha affermato che le suddette prove eludono il divieto espresso dall'articolo 8, legge n. 300/1970 perché coinvolgono aspetti della personalità e si presentano come strumenti potenzialmente ingannevoli a causa dell'impossibilità di conoscerne la griglia di lettura. L'Autorità Garante per la protezione dei dati personali ha dichiarato che i test attitudinali devono assicurare precise garanzie per la tutela della riservatezza dei lavoratori e la non discriminazione in base alle opinioni politiche e sindacali. Si veda il Comunicato stampa dell'11 luglio 1998 in cui il Garante invitava il Comune di Marino a sospendere ogni forma di utilizzazione e di ulteriore raccolta dei dati connessi ai test e, più recentemente, il provvedimento n. 302 del 21 luglio 2012, [doc. web. N. 1825852].

[19] Cfr. articolo 10, comma1, d.lgs. n. 276/2003

[20] PRETEROTI A., *Lavoro e previdenza*, in M. BIANCA, F.D. BUSNELLI (a cura di), *La protezione dei dati personali: commentario al d.lgs. 30 giugno 2003, n. 196*, Cedam Padova, *2007*, p. 1467;
LAMBERTUCCI P., *svolgimento del rapporto di lavoro e tutela dei dati personali*, *in* CARINCI F., DE LUCA TAMAJO R., TOSI P., TREU T. (a cura di), *La tutela della privacy del lavoratore*, in *Quad. dir. Lav. rel. ind*., 24, 2000, pp. 61 ss.

[21] CARINCI M.T., *Il controllo a distanza dei lavoratori dopo il "Jobs Act" (art. 23, D.lgs. 151/2015) spunti per un dibattito, in Labour and Law Issues, 2016*, 1, p. V.

subordinato al di fuori "degli uffici e più in generale dei luoghi di lavoro"[22], comporta nuove ed ulteriori possibilità per il datore di lavoro di controllare a distanza l'attività lavorativa. Sarebbe possibile conoscere, ad esempio, l'orario a cui viene effettuato l'accesso al sistema aziendale o semplicemente geo localizzare il dipendente. Il rinvio all' articolo 4 dello Statuto dei lavoratori, nella versione novellata dall' articolo 23, del d.lgs. n. 151/2015, costituisce unitamente alle norme che disciplinano la materia della privacy la rete di tutele che il legislatore ha predisposto a protezione della sfera giuridica di riservatezza del lavoratore sul luogo di lavoro[23]. Nel corso degli anni, l'articolo 4 è stata la norma statutaria che, più di ogni altra, a subito il progresso tecnologico. Le innovazioni elettroniche sono entrate nella quotidianità del lavoro imponendo un cambio di passo che ha richiesto l'intervento del garante[24] affinchè la norma nel tempo non fornisse una lettura distorta delle tutele a protezione del patrimonio aziendale e della libertà e dignità del lavoratore. Si è andata sviluppando la categoria dei c.d. "controlli difensivi", accertamenti occulti volti a verificare illeciti penalmente rilevanti commessi dal lavoratore. È necessario sottolineare che nella definizione non trovano spazio i controlli volti al diretto accertamento dell'esecuzione dell'attività lavorativa[25]. La riforma del 2015 è intervenuta modificando la norma statutaria il cui testo, oggi, non presenta più il divieto generale di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dei lavoratori, bensì si compone di un duplice nucleo normativo. Il primo formato dai commi 1 e 2, dell'articolo 4 legge n. 300/1970, individua le autorizzazioni da ottenere per procedere all' installazione degli impianti audiovisivi e degli altri strumenti di controllo a distanza, nonché la finalità d'uso ed i limiti imposti a questi ultimi[26]. Il secondo, novità rispetto al passato, disciplina l'utilizzabilità delle informazioni raccolte "a tutti fini connessi al rapporto di lavoro a condizione che sia data al lavoratore

[22] INGRAO A., *Il controllo a distanza effettuato mediante Social network, in Labour & Law Issues*, 2016, 1, p. 105.

[23] PERRONE F., *La tutela della privacy sul luogo di lavoro: il rinnovato dialogo tra Corte Europea dei Diritti dell'Uomo e giurisdizione nazionale la sentenza Barbulescu 2, il Labor*, 2018, 3, pp. 283 ss; per un'analisi dei recenti orientamenti giurisprudenziali della Corte Europea dei Diritti dell'Uomo si veda: DALLACASA M., *controlli su strumenti informatici dopo la sentenza Barbulescu del 207 della Cedu*, in Lav. Giur., 2018, 5, pp 437 ss.

[24] Tra i provvedimenti emessi dal Garante aventi ad oggetto l'utilizzo di strumenti informatici quali mezzi di controllo del lavoratore ricordiamo: "Linee Guida per posta elettronica ed internet nel rapporto di lavoro" [doc. web. N. 1387522] adottate in data 1° marzo 2007, che forniscono suggerimenti al fine di prevenire il rischio di utilizzi impropri attraverso la valutazione *ex ante* dell'impatto che l'installazione delle apparecchiature può vere sui diritti dei lavoratori, e dell'adozione di misure tecnologiche volte a minimizzare l'uso di dati identificativi. Inoltre, con provvedimento del 2 aprile 2009 [doc. web. N. 1606053] il Garante si è pronunciato in relazione al caso di memorizzazione delle pagine *web* visitate dal lavoratore. L'installazione di un software appositamente configurato per tracciare in modo sistematico e continuativo gli accessi ad Internet del lavoratore viola la disposizione contenuta nell'articolo 4, legge n. 300/1970. Con provvedimento n. 303 del 13 luglio 2016 [doc. web. 5408460] l'Autorità Garante ha dichiarato l'illecito utilizzo di software che consentono di monitorare e tracciare gli accessi ad Internet o al servizio di posta elettronica quando l'insieme dei programmi che gestiscono l'elaboratore opera in modalità occulta e del tutto indipendente dall'attività dell'utilizzatore.

[25] Cfr. Cass. 9 luglio 2008 n. 18821, in *Giust. Civ. Mass.*, 2008, 7-8, pp.1113 ss.; in tema di controlli del datore di lavoro, in ordine agli illeciti commessi dal lavoratore che non riguardano il mero inadempimento della prestazione lavorativa ma incidono sul patrimonio aziendale, la pronuncia statuisce la legittimità dei controlli occulti posti in essere dai dipendenti dell'agenzia investigativa incaricata dal datore di lavoro.

[26] Cfr. Articolo 4, legge n. 300/1970, commi 1-2, "1. Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza 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, in caso di imprese con unità produttive ubicate in diverse provincie 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. 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".

adeguata informazione delle modalità d'uso degli strumenti e di effettuazioni dei controlli e nel rispetto di quanto disposto"[27] dal Codice della privacy. L'attuale testo normativo prevede, 5 limiti all'installazione ed all'uso di strumenti che consentono il controllo a distanza del lavoratore. In primis affinché il controllo a distanza risulti legittimo è necessario che risulti strumentale ossia persegua le finalità elencate nel primo comma dell'articolo 4, legge n. 300/1970. Il monitoraggio delle attività lavorative deve tutelare le esigenze organizzative, produttive e di sicurezza del lavoro, alle quali si aggiunge la difesa del patrimonio aziendale. Il secondo limite riguarda la procedura prevista dal legislatore per evitare che i controlli siano posti in essere all'insaputa della parte controllata. L'accordo sindacale deve risultare in forma scritta e non tacita[28] o in mancanza l'autorizzazione dell'Ispettorato del lavoro. In nessun caso, il datore di lavoro può concludere un accordo direttamente con i dipendenti. Il terzo limite si incontra nella distinzione tra strumenti di controllo e strumenti di lavoro. Sul punto, l'Ispettorato nazionale del lavoro si è espresso affermando che per strumenti di lavoro si devono considerare "quegli apparecchi, dispositivi, apparati e congegni che costituiscono un mezzo indispensabile al lavoratore per adempiere la prestazione lavorativa dedotta in contratto, e che per tale finalità siano posti in uso e messi a sua disposizione"[29]. Diversamente, per l'installazione di strumenti di controllo su dispositivi diversi dagli strumenti di lavoro è richiesto il rispetto delle indicazioni descritte al comma 1 dell'articolo 4, legge n. 300/1970. Il rispetto del quarto limite prevede che il datore di lavoro proceda ad informare adeguatamente il lavoratore finché egli possa conoscere le modalità di controllo utilizzate in azienda. Infine, l'ultimo limite riguarda il rispetto della disciplina contenuta nel d.lgs. n. 196/2003 poiché l'utilizzo delle informazioni raccolte attraverso l'impiego di strumenti di controllo prevede il trattamento dei dati personali del lavoratore.

- Con riferimento al rapporto di lavoro domestico, telelavoro e lavoro agile, il datore di lavoro deve garantire al lavoratore il rispetto della sua personalità e della sua libertà morale. L'articolo 9, comma 1, lett. h) d. lgs. n. 101/2018 ha provveduto a sostituire l'originaria rubrica dell'articolo 115 del d.lgs. 196/2003 con l'attuale "Telelavoro, lavoro agile e lavoro domestico". Il nuovo disposto dell'articolo, prevede che "nell'ambito del rapporto di lavoro domestico del telelavoro e del lavoro agile, il datore di lavoro è tenuto a garantire il rispetto

[27] Cfr. articolo 4, comma 3, legge n. 300/1970.
[28] Cass. 13 maggio 2016, n. 9904, in www.ilgiuslavorista.it, nota SESSA; Cass. 1° ottobre 2012, n. 16622; Cass. 17 luglio 2007, n 15892.
[29] Cfr. Circ. INL 7 novembre 2016, n. 2. Nello specifico, la circolare si riferiva all'installazione di apparecchiature di localizzazione satellitare GPS; l'Ispettorato nazionale del lavoro ha ritenuto che "i sistemi di geolocalizzazione rappresentino un elemento aggiuntivo agli strumenti i lavoro, non utilizzati in via primaria ed essenziale per l'esecuzione dell'attività lavorativa ma, per rispondere ad esigenze ulteriori di carattere assicurativo, organizzato, produttivo o per garantire la sicurezza del lavoro". Sul punto è intervenuto anche il Garante con la decisione del 13 luglio 2016 [doc. web. N. 5408460] che, nel tentare una tipizzazione degli strumenti utilizzati dal lavoratore vi avrebbe fatto rientrare il servizio di posta elettronica e di accesso ad Internet; il sistema di *logging* per l'esercizio del servizio di posta elettronica, i sistemi di filtraggio antivirus e quelli di inibizione automatica della consultazione di contenuti in rete. Con la decisione del 26 gennaio 2018 [doc. web. 7554790], inoltre, il Garante si è espresso a favore della raccolta di dati di fatturazione e del dettaglio chiamate relativi ai cellulari aziendali in uso ai dipendenti; tuttavia, in questo caso specifico la società aveva concluso un accordo sindacale che escludeva la possibilità di utilizzare i dati raccolti con finalità disciplinari.

della sua personalità della sua libertà morale". Il lavoratore domestico è tenuto a mantenere la necessaria riservatezza per tutto quanto si riferisce alla vita familiare. Il lavoro domestico si sostanzia in un'attività lavorativa prestata esclusivamente per il funzionamento della vita familiare del datore di lavoro ed ha per oggetto la prestazione di servizi di carattere domestico diretti al funzionamento della vita familiare. Per quanto riguarda il telelavoro ed il c.d. "lavoro agile", entrambe le tipologie contrattuali prevedono l'utilizzo di strumenti di lavoro potenzialmente idonei a fornire al datore di lavoro, la possibilità di controllare, in modo continuativo, l'attività del lavoratore con rischio di realizzare una compressione dell'interesse della propria dignità personale. Nei rapporti di lavoro privato, il legislatore non ha previsto una disciplina legale del telelavoro, bensì una regolamentazione contenuta in accordi collettivi che identifica la fattispecie contrattuale della prestazione lavorativa resa da un luogo esterno all'azienda, "avvalendosi di un computer o di un altro dispositivo mobile collegato con il sistema informatico aziendale"[30]. Il lavoro agile, stante la definizione dell'articolo 18, legge n. 81/2017, si caratterizza con la presenza di un accordo tra le parti, per il parziale svincolo dai normali parametri spazio-temporali tipici della prestazione lavorativa subordinata che per l'utilizzo "possibile" di strumenti tecnologici[31]. L'accordo tra le parti, risultante da forma scritta e relativo alla modalità di lavoro agile regola l'esercizio del potere di controllo e disciplinare del datore di lavoro sulla prestazione resa all'esterno dei locali aziendali.

- Gli istituti di patronato ed assistenza sociale, nell'ambito del mandato conferito dall' interessato, possono accedere alle banche di dati degli enti eroganti le prestazioni, in relazione a tipi di dati individuati specificamente con il consenso manifestato dall' interessato medesimo. Il Ministro del lavoro e delle politiche sociali stabilisce con proprio decreto le Linee Guida di apposite convenzioni da stipulare tra gli istituti di patronato e di assistenza sociale e gli enti eroganti le prestazioni. L'articolo 116, del d.lgs. 196/2003, rubricato "Conoscibilità di dati su mandato dell'interessato", è stato interessato da un'unica modifica al primo comma, ad opera dell'articolo 9, comma 1, lett. i), in virtù dell'abrogazione dell'articolo 23 del Codice della privacy. Il testo normativo risulta aggiornato come segue" per lo svolgimento delle proprie attività gli istituti di patronato e di assistenza sociale, nell'ambito del mandato conferito dall' interessato, possono accedere alle banche di dati degli

[30] SANTORO-PASSARELLI G., *Il lavoro autonomo non imprenditoriale, il lavoro agile e il telelavoro*, in *Riv. it. Dir. Lav*. 2017, 3, p.383.
[31] È bene ricordare che in tema di controlli su strumenti informatici, la giurisprudenza della CEDU si è pronunciata sulla delicata questione del limite al potere del datore di lavoro di controllare la corrispondenza scambiata dal lavoratore attraverso l'internet aziendale nel corso dell'orario di lavoro. La Corte ha rilevato che la necessità della password per accedere alla posta elettronica equivale alla chiusura della busta cartacea e che solo i possessori legittimi della password possono prendere visione del contenuto della corrispondenza. Cedu, 12 gennaio 2016, n. 61496, in *Riv. it. Dir. Lav., 2016, 2, II, pp. 279 ss.*

enti eroganti le prestazioni, in relazione a tipi di dati individuati specificatamente con il consenso manifestato dall' interessato medesimo".

CAPITOLO II
COVID-19 E PROTEZIONE DEI DATI PERSONALI

1. La pandemia da COVID-19 e la privacy

Il coronavirus è giunto silenzioso e terribile in Europa e nel resto del mondo, in poche settimane in gennaio 2020, cambiando la vita di milioni di persone, sino all'esito estremo della morte per molte centinaia di migliaia. Dai telegiornali e social media che ci raccontavano la lontana epidemia asiatica siamo passati a sperimentare su noi stessi la vastità della tragedia: l'immagine terribile delle bare portate via dall'esercito a Bergamo ha fatto rapidamente il giro del mondo. Le due metafore ricorrenti sono state, inevitabilmente, la peste e la guerra.

I sanitari e i malati sono diventati quindi l'avamposto e il fronte, i lavoratori (coloro che devono lavorare) operano nelle retrovie ma combattono per lo stesso obiettivo. L 'economia è diventata di "guerra", pezzi dell'industria si sono riconvertiti per produrre mascherine e macchinari sanitari. L'inevitabile calo della produzione e la crisi gravissima di molti settori sollecitano interventi straordinari, gli Stati approntano piani senza precedenti per sostenere con prestiti e sovvenzioni tutti i settori dell'economia e larghi strati della popolazione. Il contagio da COVID-19 produce effetti molteplici sulle regole della convivenza civile e quindi sulla costituzione e, dove esiste, sulla democrazia. Se il contagio è come una guerra allora emergenza ed eccezione sono state adottate.
Nei regimi democratici capaci di garantire il corretto funzionamento delle regole costituzionali come nel caso italiano o in altri contesti messi a dura prova subito dopo, l'emergenza è sottoposta alla dinamica di organi, procedure e atti previsti dalla Costituzione e dall'ordinamento giuridico. In Italia tutto ha avuto inizio con l'applicazione del Codice della protezione civile (D.lgs. 1/2018) e con la proclamazione dello stato di emergenza sanitaria avvenuta con delibera del Consiglio dei ministri il 31 gennaio 2020.

È poi seguita una lunga serie di atti, di varia natura giuridica, con evidenti risvolti sul piano della regolazione, del "*law enforcement*" e più ampiamente delle garanzie costituzionali e del rispetto dei diritti fondamentali, con limitazioni, divieti e sanzioni. Non sono certo mancati problemi di applicazione e numerose contraddizioni vista anche la difficoltà di coordinare, in uno Stato in cui la sanità è competenza regionale, i vari livelli di organizzazione e di gestione. Sono stati fatti "aggiustamenti" in corsa per cercare di ovviare al non agevole rapporto tra centro e periferie, tra sistema emergenziale in capo alla protezione civile e quello stabilito dalla Costituzione tramite il ricorso ai decreti-legge quali strumenti ordinari per fronteggiare in maniera complessiva i casi di necessità ed urgenza. Il diritto dell'emergenza è da ricondurre sempre ai principi fondamentali dello

Stato di diritto, in ambito nazionale ed europeo. Nell'ordinamento democratico "*necessitas habet legem*".

La pandemia è quindi stato un banco di prova importante sotto molti profili, ivi compreso quello della privacy. Su questo terreno si è, infatti, riproposto il conflitto, dalle antiche radici, tra persona e Stato, libertà e autorità, norma ed emergenza, in forme tuttavia rese del tutto inedite e più complesse dall' irrompere nei termini di questo rapporto, delle dimensioni spazio-temporali. Il contemperamento del diritto alla privacy col diritto alla salute è emerso in tutta la sua problematicità con l'esplosione dell'emergenza sanitaria dovuta alla diffusione del virus COVID-19. La gestione dei dati personali, delle numerosissime persone colpite dalla pandemia e da difendere con misure contenitive ad hoc in modo da arginare il diffondersi di questo flagello, a vario titolo da parte di tutti i soggetti pubblici e privati coinvolti in questa operazione, non è stata una questione di poco conto. A tal proposito si indicano, a titolo esemplificativo e non esaustivo, oltre ai dati relativi ai soggetti defunti, alle iniziative per il contenimento del contagio come i dati di misurazione della temperatura corporea per ottenere l' accesso in azienda o presso uffici ed esercizi commerciali, i dati sull' ubicazione contenuta nelle varie autocertificazioni o i dati trattati attraverso applicazioni che potessero consentire il tracciamento digitale dei contatti mediante l' interazione dei dispositivi mobili. Il diffondersi della pandemia ha comportato la decisione di limitare alcune libertà fondamentali delle persone e tra queste anche il fondamentale diritto "di libertà" alla protezione dei dati personali.

Le ordinanze adottate dalle competenti autorità sono state molteplici, tuttavia la normativa di riferimento è contenuta nell' art.17 bis del Decreto Legislativo 17 marzo 2020, n.18, convertito in Legge 24 aprile 2020, n.27 (cosiddetto Cura Italia). Tale articolo contiene le disposizioni sul trattamento dei dati personali nel contesto emergenziale e fissa alcuni principi generali validi fino al termine dello stato emergenziale. In primis è stabilito che determinati soggetti – quali la Protezione civile, il Ministero della Salute e l'Istituto Superiore di Sanità, le strutture pubbliche e private del Servizio sanitario nazionale– possono trattare e scambiare tra loro i dati sanitari e i dati relativi a condanne penali e reati, purché i trattamenti siano necessari all' espletamento delle funzioni loro attribuite nell'ambito dell'emergenza sanitaria (comma 1).

Il legislatore giustifica tale possibilità di trattamento richiamando motivi di interesse pubblico nel settore della sanità pubblica e, in particolare, la finalità di "garantire la protezione dall' emergenza sanitaria a carattere transfrontaliero determinata dalla diffusione del COVID-19 mediante adeguate misure di profilassi", nonché di "assicurare la diagnosi e l'assistenza sanitaria dei contagiati ovvero la gestione emergenziale del Servizio sanitario nazionale". Nell' autorizzare tale trattamento, la disposizione ribadisce la complementarietà tra la normativa italiana e quella europea in materia di protezione dei dati personali, che si applica anche in questo particolare regime transitorio. Infatti, è

precisato che il trattamento avviene nel rispetto dell'art. 9, par.2, lett. g), h), e i), e dell'art. 10 del regolamento europeo UE/2016/679 nonché dell'art. 2 sexies, comma 2, lett. t) e u), del Codice della privacy.

Nel caso di comunicazioni di dati personali nei confronti di soggetti, pubblici e privati, diversi da quelli espressamente individuati nonché di diffusione degli altri dati personali, diversi da quelli di cui all' art.9 (trattamento di speciali categorie di dati) e art.10 (trattamento di dati personali relativi a condanne penali e reati) del GDPR, sono previsti limiti più stringenti. In merito il legislatore stabilisce che le dette operazioni siano effettuate laddove risultino indispensabili ai fini dello svolgimento delle attività connesse alla gestione dell'emergenza sanitaria (comma 2). I trattamenti di dati personali, sia quelli di cui al comma 1 che quelli al comma 2 della norma, in ogni caso, devono essere effettuati nel rispetto dei principi indicati nell' art. 5 (vedasi Cap. 1 par.1.3.3) del GDPR, adottando misure appropriate a tutela dei diritti e delle libertà degli interessati. I commi successivi dell'art.17 bis individuano una disciplina specifica valida per le sole autorità competenti individuate al comma 1, semplificando gli adempimenti previsti dalla normativa generale. Tali enti potranno designare i soggetti autorizzati al trattamento con modalità semplificate, anche in via orale e decidere di omettere l'informativa o di fornire un'informativa semplificata, previa comunicazione orale agli interessati dalla limitazione. Tenuto conto della natura transitoria delle regole individuate, gli enti indicati al termine dello stato di emergenza devono adottare misure idonee a ricondurre i trattamenti di dati personali effettuati in questo particolare contesto all' ambito delle ordinarie competenze e delle regole che disciplinano i trattamenti di dati personali.

2. Trattamento dei dati relativi alla salute in ambito sanitario in condizione di emergenza sanitaria

Il trattamento di "categorie particolari di dati personali" (art.9 del GDPR), tra i quali rientrano i dati relativi alla salute, è in via generale, vietato a meno che il titolare, dimostri di soddisfare almeno una delle condizioni previste dall' art.9, par.2 del GDPR. Le eccezioni previste dall'art.9 del GDPR sono riconducibili ai trattamenti necessari per:

a) motivi di interesse pubblico rilevante sulla base del diritto dell'UE o degli Stati membri (art.9, par.2, lett. g) del GDPR;
b) motivi di interesse pubblico nel settore della sanità pubblica, 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 preveda misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale (art.9 par.2

lett. i) del GDPR e considerando n.54) (es. emergenze sanitarie conseguenti a sismi e sicurezza alimentare);

c) finalità di cura, e cioè finalità di medicina preventiva, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione/Stati membri o conformemente al contratto con un professionista della sanità, (art.9, par.2 lett. h) e pra.3 del GDPR e considerando n. 53.

Il consenso dell'interessato al trattamento dei dati non è richiesto per i trattamenti essenziali per finalità determinate e connesse alla cura della salute ed effettuati da un professionista sanitario soggetto al segreto professionale (o altra persona soggetta all' obbligo di segretezza). Tra i trattamenti non rientranti nelle ipotesi suddette e che richiedono esplicito consenso dell'interessato (art.9. par.2, lett. a), un esempio è il caso dei trattamenti effettuati attraverso il Fascicolo sanitario elettronico ed i trattamenti connessi all'utilizzo di App mediche, con le quali autonomi titolari raccolgono dati, anche sanitari dell'interessato, per finalità diverse dalla telemedicina, o quando, ai dati dell'interessato possono avere accesso soggetti diversi dai professionisti sanitari o da altri soggetti tenuti al segreto professionale. In base al principio di trasparenza (art. 5 del GDPR), i titolari devono informare l'interessato sui principali elementi del trattamento.

Per i tempi di conservazione, invece, se non fissati da specifiche norme, sono definiti dal titolare ed in ogni caso devono essere indicati nella informativa, anche attraverso i criteri utilizzati per determinarli (art.13 e 14 del GDPR). Risulta, obbligatorio la tenuta del Registro dei trattamenti e la nomina di un DPO per gli organismi pubblici e nel caso di trattamenti in larga scala. Quest' ultimo è anche il caso di trattamenti dati relativi a pazienti svolto da un ospedale privato, da una casa di cura o da un'assistenza sanitaria assistenziale. Nella situazione di emergenza sanitaria, come il caso della pandemia in corso, l'attività di trattamento ricade nell' ipotesi prevista dall' art. 9 par.2 lett. i) del GDPR per cui risulta applicabile la deroga al generale divieto di trattare "categorie particolari di dati" quando: «il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, 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».

Infatti, il decreto-legge 9 marzo 2020, n. 14 recante Disposizioni urgenti per il potenziamento del Servizio sanitario nazionale in relazione all' emergenza COVID-19 in vigore dal 10 marzo

2020, consente una disciplina semplificata per la tutela dei dati personali, in base al suddetto art. 9 par.2 lett. i) del GDPR.

3. Protezione dei dati sanitari nella pandemia COVID-19

Il regime del trattamento dei dati nell'attuale emergenza sanitaria da COVID-19, è regolato dall'articolo 14 decreto-legge 9 marzo 2020 (diventato poi art. 17 bis del decreto-legge 18/2020 convertito in legge 24 aprile 2020, N. 27). Tale articolo 14 ha in primis posto il carattere temporaneo del regime semplificato, con vigenza non superiore alla durata dello stato di emergenza. Ha quindi previsto che:

a) i dati personali, comuni e "sensibili" possono essere trattati ed avere una circolazione interna agli organi deputati al contrasto dell'emergenza, tra essi rientrano anche "gli uffici del Ministero della salute e dell'Istituto Superiore di Sanità, le strutture, pubbliche e private, che operano nell'ambito del Servizio Sanitario Nazionale ed i soggetti deputati a monitorare e a garantire l'esecuzione delle misure disposte ai sensi dell'articolo 3 decreto legge 20/02/2020 n. 6";
b) i medesimi dati trattati possono essere comunicati ad altri soggetti pubblici e privati nonché diffusi qualora ciò risulti indispensabile al fine dello svolgimento delle attività connesse alla gestione dell'emergenza in atto;
c) i principi generali contenuti nell'articolo 5 GDPR (a titolo esemplificativo e non esaustivo liceità, correttezza, trasparenza, finalità, minimizzazione) si applicano al trattamento;
d) il conferimento di incarichi di trattamento ai sensi dell'art. 2 *quaterdecies* del codice in materia di protezione dei dati potrà avvenire con modalità semplificate, ed anche oralmente;
e) le autorità sanitarie e gli altri soggetti autorizzati, qualora trattino dati raccolti presso l'interessato, possono omettere o rendere in forma semplificata l'informativa descritta dall'art. 13 GDPR.

Il fine della disciplina "semplificata" della tutela dei dati personali nell' emergenza sanitaria è agevolare e velocizzare lo scambio di informazioni tra le autorità sanitarie, sviluppando così la sorveglianza territoriale e rendendo efficace il contenimento dell'epidemia. In riferimento al sistema della sorveglianza sono rilevanti i seguenti provvedimenti che hanno inciso sulla disciplina dei titolari del trattamento, la tipologia dei dati raccolti e la direzione del flusso comunicativo.

Il primo dei provvedimenti è l'ordinanza del Ministero della Salute, del 21 febbraio 2020 concernente la sorveglianza dei soggetti a rischio contagio. Secondo l'art.2 i dati personali raccolti nell' ambito dell' attività di sorveglianza e, dunque, in base all' art. 1, in caso di quarantena con

sorveglianza attiva per soggetti che abbiano avuto contatti stretti con casi confermati di infezione "vengono trattati dall' Autorità sanitaria competente per motivi di interesse pubblico nel settore della sanità pubblica, ai sensi dell'art.9, paragrafo 2, del Regolamento UE 2016/679, nel rispetto delle disposizioni vigenti in materia di protezione dati personali, ivi incluse quelle relative al segreto professionale, e in relazione al contesto emergenziale in atto".

L' ordinanza del Dipartimento di protezione civile del 27 febbraio 2020 ha, invece attribuito all' Istituto Superiore di Sanità (ISS) la sorveglianza epidemiologica e quella microbiologica del SARS-CoV-2, disponendo la creazione di una piattaforma informatica nella quale devono confluire i dati raccolti da tutte le Regioni e le Province Autonome di Trento e Bolzano. L' ordinanza prevede che l'ISS raccolga i campioni biologici positivi di tutte le persone sottoposte a sorveglianza epidemiologica per analizzarli, per confermare i dati di positività e tenerne una lista aggiornata.
I DPCM del 4 ed 8 marzo 2020 stabiliscono per i soggetti che abbiano soggiornato in zone a rischio l'obbligo di comunicare tali informazioni all'azienda sanitaria competente per il territorio, nonché al medico di medicina generale.

Il decreto-legge 8 aprile 2020 n.23 che con il suo art.40 ha previsto che limitatamente al periodo dello stato di emergenza, "al fine di migliorare la capacità di coordinamento e di analisi delle evidenze specifiche disponibili sui medicinali, l'AIFA (Agenzia Italiana del Farmaco) può accedere a tutti i dati degli studi clinici sperimentali, osservazionali e dei programmi di uso terapeutico compassionevole, per pazienti con COVID-19".

Il Garante della protezione dei dati personali ha chiarito, a tal proposito, nella sezione FAQ[32] relativa al Trattamento dati nel contesto delle sperimentazioni cliniche e delle ricerche mediche nell'ambito dell'emergenza sanitaria da COVID-19, che i centri di sperimentazione possono trattare dati personali, anche relativi alla salute dei pazienti affetti da COVID-19 per sperimentazioni cliniche dei medicinali, nella misura necessaria per il contrasto della pandemia, sulla base del consenso degli interessati o di un altro presupposto giuridico ai sensi dell' art.9, par.2 del GDPR, in conformità al diritto dell' Unione o nazionale per motivi di interesse pubblico rilevante, per motivi di interesse pubblico nel settore della sanità pubblica e per fini di ricerca scientifica. Nel caso di impossibilità di informare gli interessati ed acquisire il consenso, i titolari del trattamento devono raccogliere tale consenso, previa informativa, presso chi esercita legalmente la potestà di questi ultimi, da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato.

[32] FAQ (Frequently Asked Questions) – Domande Frequenti

In questo scenario emergenziale, e del tutto nuovo, è importante evidenziare che il Comitato europeo per la protezione dei dati (*European Data Protection Board* - EPDB) ha adottato il 21 aprile 2020 le linee guida sul trattamento dei dati relativi alla salute per finalità di ricerca nel contesto dell'emergenza legata al COVID-19. Le Linee Guida chiariscono che il GDPR contiene numerose disposizioni in merito al trattamento dei dati relativi alla salute per finalità di ricerca scientifica, applicabili anche nel cotesto pandemico. Tali Linee Guida richiamano il necessario rispetto dell'art. 5 del GDPR e dei suoi principi in particolare la trasparenza, la limitazione delle finalità, la minimizzazione dei dati e limiti alla conservazione, l'integrità e a riservatezza. Data la necessaria condivisione internazionale dei dati personali relativi alla salute per finalità di ricerca scientifica, le Linee Guida fanno riferimento al capo V del GDPR sul trasferimento dei dati, in particolare art.45 per cui il trasferimento è ammesso se la Commissione ha deciso che il paese terzo o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato. L' EPDB ha inoltre affermato che il quadro giuridico in materia di protezione dei dati "è stato concepito per essere flessibile, in quanto tale, è in grado di conseguire una risposta efficace per limitare la pandemia e proteggere i diritti umani e le libertà fondamentali". Per il Comitato il trattamento automatizzato dei dati e le tecnologie digitali possono essere elementi chiave nella lotta alla pandemia. Esso, chiarisce, la necessità di "guardarsi dal rischio di effetti irreversibili": le misure adottate devono essere al solito necessarie, limitate nel tempo, di portata minima e revisionate periodicamente. Viene inoltre chiarito che le esigenze di contrasto all'epidemia e la tutela della salute pubblica, possono essere considerate possibili basi giuridiche del trattamento alternative al consenso degli interessati, sia per i dati comuni, che per i dati particolari.

Per l'uso di App per la lotta al virus, il Comitato europeo per la protezione dei dati ha stabilito che "il monitoraggio sistematico su larga scala dell'ubicazione e/o dei contatti tra persone fisiche costituisce una grave interferenza nella vita privata, solo facendo affidamento su un'adozione volontaria da parte degli utenti per ciascuno dei rispettivi scopi" tale azione può essere considerata legittima posto che le persone che non intendono o non possono utilizzare tali applicazioni non devono subire alcun pregiudizio. Il Comitato in riferimento all'utilizzo dei dati relativi all'ubicazione, afferma che sarebbe da privilegiare il trattamento dei dati anonimi piuttosto che i dati personali.

4. Profili applicativi sulla protezione dei dati nella pandemia COVID-19 nel contesto lavorativo

Con riferimento al trattamento dei dati personali in ambito lavorativo, il 14 marzo 2020 è stato sottoscritto il protocollo di sicurezza anti-contagio adottato ai sensi dell'art.1, n.7, lett. d) del D.P.C.M 11 marzo 2020 integrato poi dal protocollo del 24 aprile 2020, successivamente aggiornato con la versione del 6 aprile 2021 attraverso l'ordinanza del 21 maggio 2021, con la quale il Ministro della

Salute, di concerto con il Ministro del Lavoro ha disposto che il protocollo nella versione aggiornata del 6 aprile 2021, aggiorna e sostituisce la versione del 24 aprile 2020.

Nell'attuale situazione legata all' emergenza epidemiologica, i datori di lavoro, quindi, al fine di contenere il contagio, sono tenuti ad osservare le misure per il contenimento e la gestione dell'emergenza contenute nel suddetto "Protocollo condiviso di regolamentazione delle misure per il contrasto ed il contenimento del COVID-19 negli ambienti di lavoro" tra Governo e parti sociali dal 14 marzo 2020. Il documento è stato realizzato per agevolare gli enti e le imprese nell' adozione di protocolli di sicurezza anti-contagio, negli ambienti di lavoro, contenendo importanti disposizioni anche in materia privacy.

La rilevazione in tempo reale della temperatura corporea del lavoratore, associata all' identità dell'interessato, costituisce un trattamento di dati personali, e quindi deve avvenire ai sensi della disciplina privacy vigente. Non è ammessa la registrazione del dato relativo alla temperatura corporea rilevata, bensì è possibile identificare l'interessato solo qualora sia necessario a documentare le ragioni che hanno impedito l'accesso ai locali. Nel caso in cui la temperatura venga rilevata a clienti o visitatori occasionali, anche se superiore alla soglia indicata nelle disposizioni emergenziali, non è necessario registrare il dato concernente il motivo del diniego di accesso. Nel rispetto della disciplina privacy, occorre fornire l'informativa sul trattamento dei dati personali. Tale informativa può omettere le informazioni di cui l'interessato è già in possesso e può essere fornita anche oralmente.
Quanto ai contenuti dell'informativa stessa, come finalità può essere indicata la prevenzione dal contagio da COVID-19 e come base giuridica può essere indicata l'implementazione dei protocolli di sicurezza anti-contagio ai sensi dell'art.1, n.7, lett. d) del D.P.C.M. 11 marzo 2020. Per la conservazione dei dati si può far riferimento al termine dell'emergenza. Risulta inoltre fondamentale definire le misure tecniche e organizzative adeguate a proteggere i dati. Sotto il profilo organizzativo, occorre individuare i soggetti preposti al trattamento e fornire loro le istruzioni necessarie. I dati possono essere trattati esclusivamente per finalità di prevenzione da contagio da COVID-19 e non devono essere diffusi e comunicati a terzi fuori delle specifiche previsioni normative. In caso di isolamento temporaneo dovuto al superamento della soglia di temperatura, occorre assicurare modalità tali da garantire la riservatezza e la dignità del lavoratore. Le stesse garanzie occorre assicurarle anche nel caso in cui il lavoratore comunichi all' ufficio responsabile del personale di aver avuto, al di fuori del contesto lavorativo, contatti con soggetti risultati positivi e nel caso di allontanamento del lavoratore che durante l'attività lavorativa sviluppi febbre e sintomi di infezione respiratoria.

Secondo il Protocollo nel par.2 Modalità di Ingresso in azienda

- Il personale, prima dell'accesso al luogo di lavoro potrà essere sottoposto al controllo della temperatura corporea. Se tale temperatura risulterà superiore ai 37,5°C, non sarà consentito l'accesso ai luoghi di lavoro. Le persone in tale condizione - nel rispetto delle indicazioni riportate in nota[33] - saranno momentaneamente isolate e fornite di mascherina chirurgica ove non ne fossero già dotate, non dovranno recarsi al Pronto Soccorso e/o nelle infermerie di sede, ma dovranno contattare nel più breve tempo possibile il proprio medico curante e seguire le sue indicazioni.

- Il datore di lavoro informa preventivamente il personale, e chi intende fare ingresso in azienda, della preclusione dell'accesso a chi, negli ultimi 14 giorni, abbia avuto contatti con soggetti risultati positivi al virus SARS-CoV-2/COVID-19 o provenga da zone a rischio secondo le indicazioni dell'OMS[34].

- Per questi casi si fa riferimento alla normativa di seguito richiamata e alle successive, ulteriori disposizioni che potranno essere adottate in materia: o agli articoli 14, comma 1, e 26, del decreto-legge 17 marzo 2020, n. 18, convertito, con modificazioni, dalla legge 24 aprile 2020, n. 27; o all'articolo 1, comma 1, lettera d), del decreto-legge 25 marzo 2020, n. 19, convertito, con modificazioni, dalla legge 22 maggio 2020, n. 35; o all'articolo 1 del decreto-legge 16 maggio 2020, n. 33, convertito, con modificazioni, dalla legge 14 luglio 2020, n. 74; o all'articolo 1-bis del decreto-legge 30 luglio 2020, n. 83, convertito, con modificazioni, dalla legge 25 settembre 2020, n. 124.

[33] La rilevazione in tempo reale della temperatura corporea costituisce un trattamento di dati personali e, pertanto, deve avvenire ai sensi della disciplina privacy vigente. A tal fine si suggerisce di: 1) rilevare a temperatura e non registrare il dato acquisto. È possibile identificare l'interessato e registrare il superamento della soglia di temperatura solo qualora sia necessario a documentare le ragioni che hanno impedito l'accesso ai locali aziendali; 2) fornire l'informativa sul trattamento dei dati personali. Si ricorda che l'informativa può omettere le informazioni di cui l'interessato è già in possesso e può essere fornita anche oralmente. Quanto ai contenuti dell'informativa, con riferimento alla finalità del trattamento potrà essere indicata la prevenzione dal contagio dal virus SARS-CoV-2 (COVID-19) e con riferimento alla base giuridica può essere indicata l'implementazione dei protocolli di sicurezza anti-contagio ai sensi degli articoli 4, comma 1, e 30, comma 1, lettera c), del dPCM 2 marzo 2021 e con riferimento alla durata dell'eventuale conservazione dei dati si può far riferimento al termine dello stato d'emergenza; 3) definire le misure di sicurezza e organizzative adeguate a proteggere i dati. In particolare, sotto il profilo organizzativo, occorre individuare i soggetti preposti al trattamento e fornire loro le istruzioni necessarie. A tal fine, si ricorda che i dati possono essere trattati esclusivamente per finalità di prevenzione dal contagio da SARS-CoV-2 (COVID-19) e non
devono essere diffusi o comunicati a terzi al di fuori delle specifiche previsioni normative (es. in caso di richiesta da parte dell'Autorità sanitaria per la ricostruzione della filiera degli eventuali "contatti stretti di un lavoratore risultato positivo al COVID-19); 4) in caso di isolamento momentaneo dovuto al superamento della soglia di temperatura, assicurare modalità tali da garantire la riservatezza e la dignità del lavoratore. Tali garanzie devono essere assicurate anche nel caso in cui il lavoratore comunichi all'ufficio responsabile del personale di aver avuto, al di fuori del contesto aziendale, contatti con soggetti risultati positivi al virus SARS-CoV-2 (COVID-19) e nel caso di allontanamento del lavoratore che durante l'attività lavorativa sviluppi febbre e sintomi di infezione respiratoria e dei suoi colleghi (v. infra)

[34] Qualora si richieda il rilascio di una dichiarazione attestante la non provenienza dalle zone a rischio epidemiologico e l'assenza di contatti, negli ultimi 14 giorni, con soggetti risultati positivi al virus SARS-CoV-2 (COVID-19), si ricorda di prestare attenzione alla disciplina sul trattamento dei dati personali, poiché l'acquisizione della dichiarazione costituisce un trattamento dati. A tal fine, si applicano le indicazioni di cui alla precedente nota n. 33 e, nello specifico, si suggerisce di raccogliere solo i dati necessari, adeguati e pertinenti rispetto alla prevenzione del contagio da virus SARS-CoV-2 (COVID-19). Ad esempio, se si richiede una dichiarazione sui contatti con persone risultate positive al virus SARS-CoV-2 (COVID-19), occorre astenersi dal richiedere informazioni aggiuntive in merito alla persona risultata positiva. Oppure, se si richiede una dichiarazione sulla provenienza da zone a rischio epidemiologico, è necessario astenersi dal richiedere informazioni aggiuntive in merito alle specificità dei luoghi.

- La riammissione al lavoro dopo l'infezione da virus SARS-CoV-2/COVID-19 avverrà secondo le modalità previste dalla normativa vigente (circolare del Ministero della salute del 12 ottobre 2020 ed eventuali istruzioni successive). I lavoratori positivi oltre il ventunesimo giorno saranno riammessi al lavoro solo dopo la negativizzazione del tampone molecolare o antigenico effettuato in struttura accreditata o autorizzata dal servizio sanitario.

- Qualora, per prevenire l'attivazione di focolai epidemici, nelle aree maggiormente colpite dal virus, l'autorità sanitaria competente disponga misure aggiuntive specifiche, come ad esempio l'esecuzione del tampone per i lavoratori, il datore di lavoro fornirà la massima collaborazione, anche attraverso il medico competente, ove presente.

- Al fine della prevenzione di ogni forma di affollamento e di situazioni a rischio di contagio, trovano applicazione i protocolli di settore per le attività produttive di cui all'Allegato IX al DPCM vigente.

È fatto obbligo al datore di lavoro di fornire la massima collaborazione anche attraverso il medico competente, ove presente, e di collaborare per l'attivazione delle misure di profilassi ed individuazione dei contatti stretti. Secondo le indicazioni del Ministero della Salute, il datore di lavoro dovrà adottare in caso di presenza di persona affetta all' interno dei locali, le misure relative alla pulizia e alla sanificazione.

Anche nell' emergenza, permane il divieto al medico competente di informare il datore di lavoro circa le specifiche patologie dei lavoratori. Il medico competente collabora col datore di lavoro per le misure di regolamentazione legate al COVID-19: il medico segnala al datore di lavoro situazioni di particolare fragilità e patologie attuali o pregresse dei dipendenti e, pertanto, quei casi specifichi a cui la condizione di fragilità connessa anche allo stato di salute del dipendente impongono l'impiego dello stesso in ambiti meno esposti al rischio di infezione. Al datore di lavoro non è necessario fornire informazioni sulla specifica patologia del lavoratore. Il datore di lavoro non dovrà comunicare i dati relativi al personale contagiato al Rappresentante dei lavoratori in azienda.

5. Test sierologici e Vaccinazioni nel contesto lavorativo

La trattazione dei test sierologici e gli obblighi vaccinali nel contesto lavorativo hanno richiesto profili applicativi rispetto ai quali il Garante ha fornito le indicazioni per un corretto trattamento dei dati personali da parte di pubbliche amministrazioni e imprese private. Il Garante ha chiarito attraverso FAQ i presupposti per l'effettuazione dei test sierologici per il Covid-19 sul posto di lavoro,

specificando, in particolare, che, nell'ambito del sistema di prevenzione e sicurezza, il datore di lavoro non può effettuare direttamente test sierologici per il Covid-19 ai propri dipendenti.

Il Garante ha specificato, in particolare, che, nell'ambito del sistema di prevenzione e sicurezza sui luoghi di lavoro o di protocolli di sicurezza anti-contagio, il datore di lavoro può richiedere ai propri dipendenti di effettuare test sierologici solo se disposto dal medico competente o da altro professionista sanitario in base alle norme relative all'emergenza epidemiologica. Solo il medico del lavoro, infatti, nell'ambito della sorveglianza sanitaria, può stabilire la necessità di particolari esami clinici e biologici. Il medico competente può inoltre suggerire l'adozione di mezzi diagnostici, qualora li ritenga utili al fine del contenimento della diffusione del virus, nel rispetto delle indicazioni fornite dalle autorità sanitarie, anche riguardo alla loro affidabilità e appropriatezza.

Nelle FAQ l'Autorità precisa anche che le informazioni relative alla diagnosi o all'anamnesi familiare del lavoratore non possono essere trattate dal datore di lavoro (ad esempio, mediante la consultazione dei referti o degli esiti degli esami). Il datore di lavoro deve, invece, trattare i dati relativi al giudizio di idoneità del lavoratore alla mansione svolta e alle eventuali prescrizioni o limitazioni che il medico competente può stabilire. Le visite e gli accertamenti, anche ai fini della valutazione della riammissione al lavoro del dipendente, devono essere posti in essere dal medico competente o da altro personale sanitario, e, comunque, nel rispetto delle disposizioni generali che vietano al datore di lavoro di effettuare direttamente esami diagnostici sui dipendenti.

Il Garante ha chiarito infine che la partecipazione agli screening sierologici promossi dai Dipartimenti di prevenzione regionali nei confronti di particolari categorie di lavoratori a rischio di contagio, come operatori sanitari e forze dell'ordine, può avvenire solo su base volontaria. I risultati possono essere utilizzati dalla struttura sanitaria che ha effettuato il test per finalità di diagnosi e cura dell'interessato e per disporre le misure di contenimento epidemiologico previste dalla normativa d'urgenza in vigore (es. isolamento domiciliare).Sempre al fine di prevenire possibili trattamenti illeciti di dati personali e di evitare inutili costi di gestione o possibili effetti discriminatori, il Garante per la privacy non si è sottratto dal fornire indicazioni utili ad imprese, enti e amministrazioni pubbliche affinché possano applicare correttamente la disciplina sulla protezione dei dati personali nel contesto emergenziale, attraverso FAQ, pubblicate sul sito istituzionale, fornendo risposte ai quesiti in riferimento ai profili applicativi in ambito vaccinazioni e datore di lavoro.

Nelle FAQ il Garante ha precisato che il datore di lavoro non può acquisire, neanche con il consenso del dipendente o tramite il medico compente, i nominativi del personale vaccinato o la copia delle certificazioni vaccinali. Ciò non è consentito dalla disciplina in materia di tutela della salute e

sicurezza nei luoghi di lavoro né dalle disposizioni sull'emergenza sanitaria. Il consenso del dipendente non può costituire, in questi casi, una condizione di liceità del trattamento dei dati, non potendo il consenso costituire in tal caso una valida condizione di liceità in ragione dello squilibrio del rapporto tra titolare e interessato nel contesto lavorativo (considerando 43 del Regolamento). Il datore di lavoro può, invece, acquisire, in base al quadro normativo vigente, i soli giudizi di idoneità alla mansione specifica redatti dal medico competente.

Il Garante ha chiarito inoltre che - in attesa di un intervento del legislatore nazionale che eventualmente imponga la vaccinazione anti Covid-19 quale condizione per lo svolgimento di determinate professioni[35], attività lavorative e mansioni - nei casi di esposizione diretta ad "agenti biologici" durante il lavoro, come nel contesto sanitario, si applicano le disposizioni vigenti sulle "misure speciali di protezione" previste per tali ambienti lavorativi (art. 279 del d.lgs. n. 81/2008). Anche in questi casi, solo il medico competente, nella sua funzione di raccordo tra il sistema sanitario e il contesto lavorativo, può trattare i dati personali relativi alla vaccinazione dei dipendenti, e tra questi, se del caso, le informazioni relative alla vaccinazione, nell'ambito della sorveglianza sanitaria e in sede di verifica dell'idoneità alla mansione specifica (art. 25, 39, comma 5, e 41, comma 4, d.lgs. n. 81/2008).

Il datore di lavoro deve quindi limitarsi ad attuare, sul piano organizzativo, le misure indicate dal medico competente nei casi di giudizio di parziale o temporanea inidoneità. Con un comunicato successivo pubblicato il 1° marzo 2021, il Garante ha ulteriormente commentato la questione dei cosiddetti "pass vaccinali", ossia il requisito della vaccinazione come precondizione per l'accesso a certi locali (non soltanto lavorativi). L'Autorità ha ribadito la necessità che il trattamento dei dati relativi allo stato vaccinale dei cittadini a fini di accesso a determinati locali o di fruizione di determinati servizi sia oggetto di una norma di legge nazionale conforme ai principi in materia di protezione dei dati personali (in particolare proporzionalità, minimizzazione e limitazione delle finalità), affinchè sia realizzato un bilanciamento tra riservatezza ed interesse pubblico. In assenza di

[35] Ai fini di completezza espositiva in termini di obbligo vaccinale e soggetti obbligati, esenzioni e termine di validità per l'art. 4, comma 1, d. l. 44 del 1° aprile 2021, "al fine di tutelare la salute pubblica e mantenere adeguate condizioni di sicurezza nell'erogazione delle prestazioni di cura e assistenza", la vaccinazione gratuita per la prevenzione dell'infezione da SARS-CoV-2 costituisce requisito essenziale per l'esercizio della professione e per lo svolgimento delle prestazioni lavorative rese dai soggetti obbligati. Soggetti obbligati sono "gli esercenti le professioni sanitarie e gli operatori di interesse sanitario" (come evidenziate/i dal Ministero della salute nel proprio sito istituzionale, in base a varie leggi, le "professioni sanitarie" sono quelle dei farmacisti, medici chirurghi, odontoiatri, veterinari, biologi, fisici, chimici, psicologi, nonché degli esercenti le professioni sanitarie infermieristiche, ostetriche, tecnico sanitarie, della riabilitazione e della prevenzione; quanto agli "operatori di interesse sanitario", si tratta di massofisioterapisti, operatori socio-sanitari, assistenti di studio odontoiatrico). Sono esclusi dall'obbligo, in quanto non rientranti in dette due categorie, gli esercenti le arti ausiliarie delle professioni sanitarie e degli operatori di interesse sanitario, in cui sono inclusi i massaggiatori capi bagnini degli stabilimenti idroterapici, gli ottici, gli odontotecnici, le puericultrici. Per essere inclusi nell'obbligo vaccinale occorre che gli appartenenti alle predette categorie svolgano la loro attività "nelle strutture sanitarie, sociosanitarie e socioassistenziali, pubbliche e private, nelle farmacie, parafarmacie e negli studi professionali. L'obbligo persisterà fino alla completa attuazione del piano strategico nazionale dei vaccini (art. 1, comma 457, Legge 178 del 30 dicembre 2020) e comunque sarà valido fino a non oltre il termine del corrente anno. Inoltre, con decreto-legge 1° aprile 2021, n.44, all' articolo 3 è stata esclusa espressamente la responsabilità penale degli operatori sanitari per eventi avversi nelle ipotesi di uso conforme del vaccino.

una tale base giuridica normativa, qualsiasi sistema che porti a distinguere i cittadini vaccinati dai cittadini non vaccinati è da considerarsi illegittimo.

In questa trattazione non possiamo non menzionare che in data 6 aprile 2021, è stato sottoscritto il "Protocollo nazionale per la realizzazione dei piani aziendali finalizzati all' attivazione dei punti straordinari di vaccinazione anti Sars-CoV-2/Covid-19 nel luoghi di lavoro". Tale Protocollo contiene le linee guida per definire ed attuare piani aziendali per la vaccinazione dei lavoratori. In coerenza con gli indirizzi del piano nazionale per la vaccinazione anti SARS- CoV-2/Covid-19 le imprese potranno organizzare la somministrazione del vaccino ai propri lavoratori rispettando regole e procedure definite nel Protocollo e nei documenti che questo richiama. La vaccinazione negli ambienti di lavoro, anche se affidata al medico competente o ad altri sanitari convenzionati con il datore di lavoro, resta un'iniziativa di sanità pubblica, per la quale è espressamente richiamato l'esonero da responsabilità del medico, previsto dal recente decreto-legge n. 44/2021, ed è evidenziato che non attiene alla disciplina della sicurezza nei luoghi di lavoro. Il Protocollo fissa linee guida nazionali per dare ulteriore contenuto al senso di responsabilità sociale mostrato dalle imprese in questa crisi pandemica, queste potranno, infatti collaborare attivamente alla realizzazione del piano vaccinale.

6. EDPB, il Garante privacy ed il contesto lavorativo nell'ambito dell'emergenza Covid-19

Il contemperamento del diritto alla privacy col diritto alla salute è emerso in tutta la sua problematicità con l'esplosione dell'emergenza sanitaria dovuta alla diffusione del virus COVID-19. Governi e organismi pubblici e privati di tutta Europa hanno adottato misure per contenere e attenuare il COVID-19, comportando il trattamento di diverse tipologie di dati personali. Non sono tardate ad arrivare le linee di indirizzo del Comitato Europeo per la Protezione dei Dati

Il Comitato Europeo per la Protezione dei Dati (EDPB) nella *Dichiarazione sul trattamento dei dati personali nel contesto dell'epidemia di COVID-19*, adottata il 19 marzo 2020 ha indicato le linee guida da seguire in termini di liceità del trattamento, con un particolare riferimento al trattamento di dati *particolari* ed alle categorie di tali dati da parte di autorità pubbliche competenti e, dedicando uno specifico paragrafo al trattamento dei dati nel contesto lavorativo, par.1.2:

Nel contesto lavorativo, il trattamento dei dati personali può essere necessario per adempiere un obbligo legale al quale è soggetto il datore di lavoro, per esempio in materia di salute e sicurezza sul luogo di lavoro o per il perseguimento di un interesse pubblico come il controllo delle malattie e altre minacce di natura sanitaria. Il RGPD prevede anche deroghe al divieto di trattamento di talune

categorie particolari di dati personali, come i dati sanitari, se ciò è necessario per motivi di interesse pubblico rilevante nel settore della sanità pubblica (articolo 9.2, lettera i), sulla base del diritto dell'Unione o nazionale, o laddove vi sia la necessità di proteggere gli interessi vitali dell'interessato (articolo 9.2.c), poiché il considerando 46 fa esplicito riferimento al controllo di un'epidemia.
Per quanto riguarda il contesto lavorativo ha precisato che:

- Il datore di lavoro può chiedere ai visitatori o ai dipendenti di fornire informazioni sanitarie specifiche nel contesto del COVID-19, applicando i principi di proporzionalità e di minimizzazione dei dati. Il datore di lavoro dovrebbe chiedere informazioni sanitarie soltanto nella misura consentita dal diritto nazionale.
- Il datore di lavoro è autorizzato a effettuare controlli medici sui dipendenti in dipendenza delle leggi nazionali in materia di lavoro o di salute e sicurezza. I datori di lavoro dovrebbero accedere ai dati sanitari e trattarli solo se ciò sia previsto dalle rispettive norme nazionali.
- Il datore di lavoro può informare colleghi o soggetti esterni del fatto che un dipendente è affetto dal COVID-19 informando il personale sui casi di COVID-19 e adottando misure di protezione; tuttavia, non si dovrebbero comunicare più informazioni del necessario. Qualora occorra indicare il nome del dipendente o dei dipendenti che hanno contratto il virus (ad esempio, in un contesto di prevenzione) e il diritto nazionale lo consenta, i dipendenti interessati ne sono informati in anticipo tutelando la loro dignità e integrità.
- Le informazioni personali trattate nel contesto del COVID-19 possono essere ottenute dai datori di lavoro nella misura necessaria a adempiere ai loro obblighi e a organizzare le attività lavorative, conformemente alla legislazione nazionale.

In linea con quanto espresso dal Comitato Europeo della Protezione dati, intervenendo nell' Audizione[36] del 13 maggio 2020 presso la Commissione 11a (Lavoro pubblico e privato, previdenza sociale) del Senato della Repubblica, il Presidente del Garante per la protezione dei dati personali si è espresso sul tema della protezione dei dati rispetto alle conseguenze che la pandemia ha determinato sul lavoro e sulle sue modalità di svolgimento da parte dei dipendenti.

Nella relazione il Presidente ha preliminarmente ribadito quanto la protezione dei dati personali dei lavoratori assume, nel contesto emergenziale, una funzione significativa, in considerazione del fatto che i lavoratori rappresentano una categoria vulnerabile e sono parti di un rapporto contrattuale, strutturalmente asimmetrico, con una controparte, e quindi in grado di condizionare anche la loro volontà. Infatti, il lavoratore ha una posizione intrinsecamente debole rispetto a quella del datore di

[36] Audizione del Presidente del Garante per la protezione dei dati personali sull'affare assegnato atto n. 453 relativo al tema Ricadute occupazionali dell'epidemia da Covid-19, azioni idonee a fronteggiare le situazioni di crisi e necessità di garantire la sicurezza sanitaria nei luoghi di lavoro

lavoro e tale differenza di potere contrattuale spesso impedisce al lavoratore di compiere le proprie scelte in modo effettivamente volontario ed autonomo. Di seguito testualmente si riporta il passo specifico: *"La disparità di potere contrattuale che connota generalmente, in senso debole, la posizione del lavoratore è tale da poterne ostacolare la reale autodeterminazione rispetto al potere datoriale, altrimenti suscettibile di esercizio, in assenza di regole adeguate, anche mediante controlli pervasivi sul dipendente. Nel contesto emergenziale che viviamo la valenza …garantista della protezione dati, in particolare in ambito lavorativo, è se possibile ancor più determinante, in ragione dell'estensione dei poteri datoriali per fini anzitutto di prevenzione dei contagi".*

Nella disamina sono stati presi in considerazione i tre aspetti di impatto fondamentale:

- I controlli dei lavoratori per prevenire il contagio
- Il tracciamento dei contatti
- Lo Smart working

Il primo aspetto è riferito ai controlli dei lavoratori effettuati sui luoghi di lavoro e finalizzati a prevenire il contagio da Covid-19. Il criterio guida nella valutazione della legittimità di tali controlli è quello per cui il trattamento dei dati personali particolari (come quelli relativi alla salute) è lecito, in presenza di esigenze di sanità pubblica, quando sussiste una previsione normativa che individua l'ambito del trattamento e soprattutto le relative garanzie.
La necessità di intervenire con urgenza, tipico di una situazione di pandemia, potrebbe portare a disattendere o comunque a non voler considerare le regole che stabiliscono le garanzie del trattamento. Nelle prime settimane della pandemia, lo stesso Garante è dovuto intervenire[37], ammonendo i datori di lavoro che raccoglievano dati sui sintomi o sui contatti dei propri lavoratori.
Fermo restando l'esigenza di tutelare i lavoratori dal rischio del contagio, le misure finalizzate a prevenire tale rischio, il rischio sanitario da cui proteggere i lavoratori, ai sensi dell'art. 2087 del codice civile oltre che del dlgs 81/08, devono garantire la protezione dei dati personali.

Le raccomandazioni indicano di limitare i trattamenti dei dati, nell' effettuazioni dei controlli dei lavoratori, nei seguenti termini:

- *la rilevazione della temperatura corporea dei dipendenti con registrazione della sola circostanza del superamento della temperatura-soglia, quando sia necessario documentare le ragioni ostative all'accesso al luogo di lavoro;*

[37] Coronavirus: Garante Privacy, 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

- *la segnalazione al datore di lavoro di provenienza da aree a rischio o di avvenuti contatti con potenziali contagiati, purché nella sola misura strettamente proporzionale all'esigenza di prevenzione e senza riferimenti nominativi a terzi;*
- *il dovere del medico competente di segnalare al datore di lavoro l'opportunità di adibire determinati lavoratori ad impieghi meno esposti al rischio infettivo, pur senza indicarne la patologia;*
- *il dovere di comunicazione, da parte datoriale all'autorità sanitaria, (ma non al Rappresentante dei lavoratori per la sicurezza o agli altri colleghi), dei nominativi dei dipendenti contagiati, collaborando alla ricostruzione della catena dei contagi e all'adozione delle misure di profilassi opportune.*

Per il trattamento delle informazioni relative al contagio dei dipendenti, il datore di lavoro, quindi, per assolvere ai propri obblighi di garantire l'incolumità dei suoi dipendenti, non è necessario che conosca l'eventuale patologia degli stessi, ma è sufficiente che abbia notizia soltanto dell'idoneità o meno del lavoratore a svolgere la prestazione lavorativa. Soltanto il medico del lavoro potrà conoscere la patologia o i relativi sintomi e conseguentemente stabilire che il lavoratore debba essere sottoposto a particolari analisi diagnostiche, come ad esempio test sierologici. Questi ultimi potranno essere disposti dal medico del lavoro che potrà conoscerne i risultati ma non potranno mai essere portati a conoscenza del datore di lavoro.

Per il tracciamento dei contagi, si ribadisce la natura esclusivamente volontaria dell'adesione al sistema di tracciamento dei contatti ed in caso di rifiuto da parte del soggetto, questi non dovrà subire alcuna conseguenza pregiudizievole.

Infine in riferimento allo *smart working*, posto che il distanziamento sociale imposto dalla situazione di pandemia ha portato i datori di lavoro ad utilizzare tale modalità di svolgimento della prestazione lavorativa, in taluni casi senza preventiva adeguata organizzazione del sistema e senza che i lavoratori fossero adeguatamente formati su tale modalità, si evidenzia che l'uso di tale sistema non può essere un modo per monitorare e controllare lo svolgimento dell' attività lavorativa del dipendente, né un modo per controllarne la localizzazione del dipendente stesso, fermo restando il riconoscimento al lavoratore in smart working del diritto alla disconnessione.

7. Trattamento dei dati dei dipendenti in risposta al COVID-19: elementi di sintesi e analisi comparata con alcuni paesi UE

Di seguito si riportano alcuni elementi di sintesi in riferimento al quadro normativo nazionale ed una tabella comparativa con 14 paesi UE ripresa da un recente lavoro di Bird & Bird (ultimo aggiornamento 8 gennaio 2021)[38].

Abbiamo visto come durante le varie fasi della pandemia i datori di lavoro si sono dovuti misurare con l'introduzione di misure per il contenimento dei contagi, finalizzato alla protezione dei dipendenti, pur mantenendo alta la capacità operativa aziendale. Tra queste, a titolo esemplificativo e non esaustivo, citiamo una serie di misure pro-contenimento dei contagi quali lo "smart working", la sanificazione sistematica degli ambienti, il tracciamento dei contagi in azienda con la previsione di misure di isolamento, le limitazioni dei viaggi di lavoro, il prelievo della temperatura in accesso alle sedi, la gestione delle entrate contingentate.

In questo scenario emergenziale abbiamo inoltre visto come la tutela della privacy del dipendente abbia dovuto ricercare punti di equilibrio non facili rispetto alla sicurezza, alla salute dei dipendenti stessi e alla necessità di garantire continuità operativa.

La dichiarazione del Comitato europeo per la protezione dei dati ("EDPB"), secondo cui le norme sulla protezione dei dati non ostacolano le misure adottate nella lotta contro il Covid-19, ha offerto poche risposte pragmatiche ai datori di lavoro che chiedevano indicazioni chiare su come rispettare tali obblighi. Nello stesso tempo a livello nazionale le autorità per la protezione dei dati sono state particolarmente caute rimandando a principi generali, lasciando ai datori di lavoro l'onere di monitorare i requisiti a livello nazionale.

Con l'obiettivo di privilegiare in uno sforzo di estrema sintesi si riportano di seguito due tabelle sinottiche in riferimento alla nostra realtà nazionale, l'Italia, la prima, con i vincoli e gli obblighi per un datore di lavoro verso i propri dipendenti, le altre categorie contrattuali ed i visitatori; nonché una seconda tabella riepilogativa generale sulle linee guida da rispettare per il contenimento dei contagi e la riapertura dei propri uffici in sicurezza:

[38] data-protection_covid-19-v03.pdf (twobirds.com)

Tabella A: COVID-19 Linee guida per il datore di lavoro in relazione alle varie categorie contrattuali di lavoratori

id	Italia - COVID-19 Linea guida per il datore di lavoro in relazione alle varie categorie contrattuali	Dipendenti	Lavoratori mobili / gig economy / agenzie di lavoro	Visitatori
1	Può il datore di lavoro richiedere se ci sono sintomi COVID-19?	**Si ma con limitazioni**: ad eccezion fatta per la raccolta dati relativi alla temperatura corporea per quanti superano la soglia dei 37,5 °C i datori di lavoro non possono richiedere i sintomi ai dipendenti! Protocollo siglato dal Governo ed i Sindacati il 24 aprile 2020: http://www.governo.it/sites/new.governo.it/files/dpcm_20201203_allegati_txt.pdf che riporta nel dettaglio tutte le misure organizzative che devono essere implementate per continuare ad operare durante il periodo di emergenza.	**Si ma con limitazioni**: ad eccezion fatta per la raccolta dati relativi alla temperatura corporea per quanti superano la soglia dei 37,5 °C i datori di lavoro non possono richiedere informazioni circa i sintomi. Se queste persone non hanno bisogno di lavorare da un luogo particolare insieme ad altri dipendenti, un datore di lavoro non può raccogliere nemmeno queste informazioni.	**No**, ad eccezion fatta per la temperatura corporea per quanti superano la soglia dei 37,5 °C in modo da bloccare l'accesso alle aree lavorative. Il datore di lavoro non può richiedere ai visitatori informazioni relative ai sintomi!
2	Può il datore di lavoro richiedere dati circa i viaggi fatti?	**Si se strettamente necessario** e fatto su base caso per caso e non per tutti i dipendenti. In caso è richiesta una dichiarazione semplice circa l'aver viaggiato in aree ad alto rischio (in Italia o all'estero). Non è possibile richiedere dettagli delle aree in cui si è viaggiato.	**Si se strettamente necessario** e fatto su base caso per caso e non per tutti gli individui. In caso è richiesta una dichiarazione semplice circa l'aver viaggiato in aree ad alto rischio (in Italia o all'estero). Non è possibile richiedere dettagli delle aree in cui si è viaggiato. Se queste persone non hanno bisogno di lavorare da un luogo particolare insieme ad altri dipendenti, un datore di lavoro non può raccogliere nemmeno queste informazioni.	**Si, ma con limitazioni**. Questo dovrebbe essere trattato come un'eccezione. Il datore di lavoro deve implementare tutte le misure organizzative indicate nel Protocollo e solo se strettamente necessario che questi visitatori debbano entrare negli uffici (ad es. personale delle pulizie, fornitori di servizi essenziali e servizi non rimandabili). In questi ultimi casi si applicano le stesse regole dei dipendenti!
3	Può il datore di lavoro richiedere di fare dei test?	**Si ma con limitazioni**. I datori di lavoro possono prendere la temperatura e se questa eccede i 37,5 °C il datore di lavoro deve registrare la motivazione dell'esclusione ad entrare al proprio posto. Non si possono effettuare altri test se non richiesti dal medico aziendale competente o da una autorità sanitaria. In caso i dati relativi alla salute possono essere trattati solo dal medico competente.	**Si ma con limitazioni**. I datori di lavoro possono prendere la temperatura e se questa eccede i 37,5 °C il datore di lavoro deve registrare la motivazione dell'esclusione ad entrare negli uffici. Se queste persone non hanno bisogno di lavorare da un luogo particolare insieme ad altri dipendenti, un datore di lavoro non può raccogliere nemmeno queste informazioni.	Solo la **lettura della temperatura per i visitatori: Si, ma solo se strettamente necessario**. Al dipendenti è richiesto prendere la temperature a quanti devono entrare negli uffici per necessità (es. servizi di pulizia, lavoratori di fornitori di servizi essenziali e/o non rimandabili).Se la temperatura eccede i 37,5 C° il datore di lavoro può registrare la ragione per cui il visitatore non può entrare nel caso in cui vi sia una ragione contrattuale per entrare.
4	Può il datore di lavoro richiedere informazioni sui sintomi dei famigliari?	**No**. Il datore di lavoro può solo richiedere se il dipendente sia stato in contatto con persone risultate positive ed eccezionalmente solo se strettamente necessario (da capire caso per caso e non può essere una misura generale). In ogni caso non si può richiedere chi sia questa persona!	**No**. Il datore di lavoro può solo richiedere se l'individuo sia stato in contatto con persone risultate positive ed eccezionalmente e solo se strettamente necessario (da capire caso per caso e non può essere una misura generale). In ogni caso non si può richiedere chi sia questa persona!	**Si, ma con limitazioni**. Questo dovrebbe essere trattato come un'eccezione. Il datore di lavoro deve implementare tutte le misure organizzative indicate nel Protocollo e solo se strettamente necessario che questi visitatori debbano entrare negli uffici (ad es. personale delle pulizie, fornitori di servizi essenziali e servizi non rimandabili). In questi ultimi casi si applicano le stesse regole dei dipendenti!
5	Si può richiedere di notificare il datore di lavoro in caso di positività al COVID-19?	**Si, ma con limitazioni**. Al dipendente è solo richiesto di notificare il datore di lavoro di sintomi durante i giorni lavorativi. I dipendenti risultati positivi devono fornire un certificato medico al datore di lavoro che mostri che il dipendente stesso sia negativo, certificato fornito in accordo alle autorità locali sanitarie competenti. E' preferibile che il certificato sia inviato al medico aziendale competente.	**Si, ma con limitazioni**. All'individuo è solo richiesto di notificare il datore di lavoro di sintomi durante i giorni lavorativi.	**No**. La notifica sarà fatta attraverso i canali ufficiali delle competenti autorità quando vengono tracciati all'indietro i contatti. Eccezione singola. se un'azienda utilizza personale esternalizzato risultato positivo al COVID-19, il soggetto deve informare l'ufficio competente dell'azienda presso cui è esternalizzato al fine di adottare le misure previste dal Protocollo ed entrambe le organizzazioni (esternalizzante ed esternalizzata) deve collaborare con l'autorità sanitaria fornendo informazioni utili per identificare eventuali contatti stretti
6	Può richiedere il datore di lavoro informazioni riguardanti l'avvenuta vaccinazione?	**Si, ma con limitazioni**. Al momento non ci sono linee guide o disposizioni legali da parte dell' Autorità Garante per la Protezione dei Dati. Come regola generale il datore di lavoro non può richiedere informazioni sui trattamenti medici (incluso il vaccino). Solo il medico aziendale competente può richiedere informazioni sulla vaccinazione del dipendente se questi dati sono rilevanti per il monitoraggio della salute del dipendente stesso. Questa informazione può essere rilevante per i dipendenti esposti a rischi di salute: i) in ordine alle condizioni di salute del dipendente (disabili, malati cronici, o seriamente ammalati). In questi casi il medico aziendale competente può richiedere se il dipendente abbia ricevuto il vaccino ed eventualmente escluderli dal proprio posto di lavoro se ritenuto pericoloso per la loro salute; ii) dovuto a specifiche condizioni di lavoro (cioè dipendenti la cui attività lavorativa non consenta il distanziamento sociale previsto o l'uso di DPI). In ogni caso quest'ultimo caso può essere alquanto controverso!	**Si, ma con limitazioni**. Al momento non ci sono linee guide o disposizioni legali da parte dell' Autorità Garante per la Protezione dei Dati. Come regola generale il datore di lavoro non può richiedere informazioni sui trattamenti medici (incluso il vaccino). Solo il medico aziendale competente può richiedere informazioni sulla vaccinazione del dipendente se questi dati sono rilevanti per il monitoraggio della salute del dipendente stesso. Questa informazione può essere rilevante per i dipendenti esposti a rischi di salute: i) in ordine alle condizioni di salute del dipendente (disabili, malati cronici, o seriamente ammalati). In questi casi il medico aziendale competente può richiedere se il dipendente abbia ricevuto il vaccino ed eventualmente escluderli dal proprio posto di lavoro se ritenuto pericoloso per la loro salute; ii) dovuto a specifiche condizioni di lavoro (cioè dipendenti la cui attività lavorativa non consenta il distanziamento sociale previsto o l'uso di DPI). In ogni	**No**. E' da notare che non ci sono leggi o linee guida fino ad oggi su questo argomento. Sembra improbabile che la legge italiana possa introdurre la possibilità per i datori di lavoro di chiedere ai visitatori queste informazioni. Secondo l'attuale quadro normativo, ai visitatori non può essere chiesto di fornire dettagli relativi alla salute, incluso se hanno già ricevuto un vaccino.
7	E' possibile per il datore di lavoro richiedere di vaccinarsi?	**No**. A meno che il Governo Italiano non stabilisca che il vaccino è obbligatorio in genere o per alcune categorie, il datore di lavoro non può imporre nessun trattamento medico se non sia mandatorio per legge. Il Governo Italiano non ha alla data del 31 Marzo 2021 emanato un obbligo generale di vaccinazione contro il COVID-19. Per cui il datore di lavoro può solo incoraggiare gli individui a vaccinarsi e non può considerare il vaccino come elemento richiesto per le attività lavorative dei propri dipendenti!	**No**. A meno che il Governo Italiano non stabilisca che il vaccino è obbligatorio in genere o per alcune categorie, il datore di lavoro non può imporre nessun trattamento medico se non sia mandatorio per legge. Il Governo Italiano non ha alla data del 31 Marzo 2021 emanato un obbligo generale di vaccinazione contro il COVID-19. Per cui il datore di lavoro può solo incoraggiare gli individui a vaccinarsi e non può considerare il vaccino come elemento richiesto per le attività lavorative degli individui in generale!	n/a
8	Si può richiedere il lavoro da casa anche se gli uffici sono aperti?	**Si**. In realtà questo è raccomandato (o mandatorio, in dipendenza del settore di attività, in accordo alla legislazione di emergenza applicabile) nel caso in cui il lavoro del dipendente si possa effettuare da remoto e che i dipendenti stessi siano dotati di adeguati strumenti di lavoro.	n/a	n/a
9	Si possono escludere dal proprio posto di lavoro i dipendenti/individui che non si siano vaccinati?	**No, a meno di particolari circostanze**. A meno che il Governo non stabilisca che il vaccino sia mandatorio in generale o per certe categorie; quindi sotto la legislazione corrente un datore di lavoro non può escludere i dipendenti dal proprio posto nel caso non siano vaccinati. Il medico aziendale competente può escludere dipendenti esposti al rischio di infezioni dovuto a particolari condizioni di salute, malattie croniche e gravi, immunodepressi, disabili nel caso non abbiano ricevuto il vaccino. Il datore di lavoro può decidere che i dipendenti che non siano stati vaccinati possano lavorare remotamente quando possibile. Il datore di lavoro può unilateralmente assegnare i dipendenti al lavoro remoto fino al 30 aprile (salvo prolungamenti estesi dal Governo stesso - aggiornamento 31 Marzo 2021). Dopo tale data, è richiesta l'autorizzazione specifica del dipendente (Accordo individuale).	**No, a meno di particolari circostanze**. A meno che il Governo non stabilisca che il vaccino sia mandatorio in generale o per certe categorie; quindi sotto la legislazione corrente un datore di lavoro non può escludere questi individui dal proprio posto nel caso non siano vaccinati. Il medico aziendale competente può escludere individui esposti al rischio di infezioni dovuto a particolari condizioni di salute, malattie croniche e gravi, immunodepressi, disabili nel caso non abbiano ricevuto il vaccino. Il datore di lavoro può decidere che gli individui che non siano stati vaccinati possano lavorare remotamente quando possibile. Il datore di lavoro può unilateralmente assegnare gli individui al lavoro remoto fino al 30 aprile (salvo prolungamenti estesi dal Governo stesso - aggiornamento 31 Marzo 2021). Dopo tale data, è richiesta l'autorizzazione specifica dell'individuo (Accordo individuale).	**No**. A meno che il Governo Italiano non stabilisca che il vaccino è obbligatorio in genere o per alcune categorie di individui.Quindi, sotto l'attuale quadro normativo un datore di lavoro non può escludere i visitatori dall'entrare nei propri uffici se non hanno fatto un vaccino.

Tabella B: linee guida, obblighi ed azioni dei datori di lavoro per evitare i contagi e riaprire i propri uffici in sicurezza

id	Italia - COVID-19 Linee Guida, Disposizioni Legali e checklist per i datori di lavoro	
1	Linee guida formali del DPA	http://www.governo.it/sites/new.governo.it/files/dpcm_20201203_allegati_txt.pdf https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9282117
2	Quali test medici può effettuare il datore di lavoro e sotto quali condizioni?	Soltanto test messi a disposizione dai programmi di monitoraggio della salute e stabiliti dal competente medico aziendale
3	Il datore di lavoro deve consigliarsi con le rappresentanze sindacali prima di prendere qualsiasi misura per il COVID-19?	Si, devono aderire al Protocollo interno basato su quanto referenziato dalla corrente legislazione di emergenza: http://www.governo.it/sites/new.governo.it/files/dpcm_20201203_allegati_txt. Pdf
4	Il datore di lavoro può tenere un registro del personale che è stato diagnosticato infetto?	Si, ma con limitazioni. Se un individuo risulta positivo durante il periodo lavorativo, il datore di lavoro può registrare questo fatto. Nessun altra lista o registrazione di dipendenti infetti può essere mantenuta.
5	Il datore di lavoro può notificare gli altri membri del personale circa un dipendente infetto da COVID-19?	No. Questo dovrebbe essere fatto dall'autorità sanitaria competente (direttamente o tramite il medico aziendale) se ritenuto rilevante secondo i protocolli sanitari approvati dalle autorità sanitarie per COVID-19 e solo per quei membri del personale a rischio di infezione.
6	Il datore di lavoro può informare gli altri membri del personale se un dipendente è morto per COVID-19? Che obblighi ci sono per un datore di lavoro in questo caso?	No. Poiché in Italia il GDPR si applica anche ai dati personali delle persone decedute, così come già chiarito nella tabella relativa ai dati sanitari del personale, il datore di lavoro non può condividere i dati di salute del personale salvo diversa disposizione dell'autorità pubblica
7	Il datore di lavoro può notificare clienti e visitatori relativamente ad un membro infetto del personale?	No. Questo dovrebbe essere fatto dalle autorità sanitarie pubbliche (direttamente o tramite il medico aziendale) se ritenuto rilevante secondo i protocolli sanitari approvati dalle autorità sanitarie per COVID-19 e solo per quei membri del personale che sono a rischio di infezione. Unica eccezione: se un'azienda utilizza personale in outsourcing risultato positivo al COVID-19, l'interessato deve informare l'ufficio competente della società in cui è affidato in outsourcing al fine di adottare le misure previste dal Protocollo ed entrambe le organizzazioni devono collaborare con le autorità sanitarie fornendo informazioni utili per identificare eventuali tracciamenti.
8	Può il datore di lavoro condividere dati sanitari con le autorità sanitarie locali per scopi di salute pubblica?	Sì. A seguito di una richiesta di un'autorità sanitaria competente, il datore di lavoro può divulgare informazioni su casi di infezione sospetti o confermati .
9	Quali passi il datore di lavoro dovrebbe considerare per la riapertura degli uffici?	In generale, si consiglia di seguire le misure previste dai Protocolli. In particolare, alla luce dell'attuale crisi epidemiologica in Italia lo smart working resta la soluzione raccomandata per quelle attività che non richiedono presenza fisica e sono compatibili con questa modalità di lavoro. Inoltre, per le aziende non compatibili con lo smart working, una volta concluse le attività di sanificazione dei locali e purché siano disponibili dispositivi di protezione individuale e obbligatorio per i lavoratori (quale equipaggiamento protettivo è necessario dipende in realtà da come il il posto di lavoro è stato riorganizzato e il tipo di lavoro di ciascun dipendente), l'organizzazione deve predisporre il rilevamento della temperatura corporea (vedere le risposte pertinenti nella tabella), si raccomanda, inoltre : di identificare un team (composto da HR, Health and safety manager (RSPP), medico aziendale e eventuale rappresentanza sindacale aziendale) per la gestione centralizzata di potenziali eventi; formalizzare le politiche interne che regolano la comunicazione interna dei dati personali relativi COVID-19; monitorare la temperatura del personale prima di entrare nei locali utilizzando termometri infrarossi o termo scanner, vietando l'accesso a chi ha la febbre superiore a 37,5 ° C; cooperare con le autorità sanitarie e rafforzare le regolari attività di monitoraggio sanitario fornito dal medico aziendale
10	E' richiesto in Italia che le persone indossino mascherine o coperture facciali?	Sì. Secondo i Protocolli, se il luogo di lavoro richiede di lavorare a una distanza interpersonale inferiore ad 1 metro e altre soluzioni organizzative non sono possibili, è comunque necessario l'utilizzo di maschere e altri dispositivi di protezione (guanti, occhiali, tute, ecc.). Quindi il personale non può rifiutarsi di indossare maschere se richiesto dal datore di lavoro. E' da notare che indossare maschere per il viso è obbligatorio anche fuori dal luogo di lavoro in alcuni ambienti (o generalmente ogni volta che qualcuno si trova in un luogo pubblico, inclusa la strada, o trasporti o altri luoghi aperti al pubblico in determinate regioni): quindi indossare maschere dovrebbe essere una prassi facilmente accettata dai dipendenti.

Infine, si riporta nella tabella C una comparazione tra quanto valido in Italia ed in alcuni paesi UE, da cui si evince come la normativa nazionale si riflette in maniera differente pur nel bilanciamento tra il dovere di proteggere e la salvaguardia della privacy dei dipendenti.

In alcuni paesi UE la normativa consente al datore di lavoro il trattamento dei dati personali incluso i dati di salute privilegiando la salvaguardia al progredire dei contagi (Slovacchia, Spagna, UK), in alcuni altri paesi la normativa consente ai datori di lavoro di avere informazioni dai loro dipendenti relativi a sintomi e viaggi tuttavia è consentito il test della temperatura solo a determinate condizioni e in ogni caso solo se strettamente necessario (Germania, Ungheria, Italia, Polonia).

Altri paesi al contrario hanno una normativa sbilanciata verso i dipendenti impedendo ai datori di lavoro di richiedere informazioni relativamente a sintomi o eseguire test di rilevamento della temperatura (Belgio, Finlandia, Francia ed Olanda). Nel caso siano confermati casi di infezioni molti paesi consentono di registrare i casi (Belgio, Danimarca, Germania, Ungheria, Slovacchia, Spagna, Svezia, UK) mentre pochi impongono restrizioni o condizioni a tali registrazioni (Repubblica Ceca, Finlandia, Francia ed Italia).

In conclusione, tenuto conto che l'approccio degli organi di governo nazionali e delle autorità di protezione dei dati si sviluppa con il progredire della pandemia, quindi paese per paese, con una recrudescenza del Covid-19 e strategie di salute pubblica sempre più diversificate, i datori di lavoro dovranno continuare ad adottare un approccio localizzato ai requisiti di privacy dei dipendenti, nonché alle più ampie implicazioni della pandemia stessa, e tenerne d'occhio gli sviluppi.

Tabella C: sintesi e comparazione Italia con alcuni paesi UE

SINTESI PAESI UE		Italy	Belgium	Czech Republic	Denmark	Finland	France	Germany	Hungary	Netherlan	Poland	Slovakia	Spain	Sweden	UK
Dipendenti	Può il datore di lavoro richiedere se ci sono sintomi COVID-19?	🟡	🟡	🟢	🟢	🟡	🔴	🟢	🟢	🔴	🟡	🟢	🟢	🟢	🟢
	Può il datore di lavoro richiedere di fare dei test?	🟡	🔴	🟡	🟡	🔴	🟡	🔴	🟡	🟡	🟡	🟡	🟡	🟢	🟢
	Si può richiedere di notificare il datore di lavoro in caso di positività al COVID-19?	🟡	🔴	🟢	🟢	🔴	🟡	🟡	🟢	🔴	🟢	🟢	🟢	🟢	🟢
	E' possibile chiedere informazioni se è stato effettuato il vaccino?	🟡	🔴	🔴	🟢	🟡	🔴	🟡	🔴	🔴	🟡	🟢	🟢	🟢	🟢
	E' possibile richiedere ai dipendenti di vaccinarsi?	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴
	E' possibile escludere dal proprio posto di lavoro dipendenti non vaccinati?	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴
Lavoratori Mobili / Gig Economy /Agenzie interinali	Può il datore di lavoro richiedere se ci sono sintomi COVID-19?	🟡	🟡	🟢	🟢	🟡	🔴	🟢	🟢	🔴	🟡	🟡	🟢	🟢	🟢
	Può il datore di lavoro richiedere di fare dei test?	🟡	🔴	🟡	🟡	🔴	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟢	🟢
	Si può richiedere di notificare il datore di lavoro in caso di positività al COVID-19?	🟡	🟡	🟢	🟢	🔴	🟡	🟡	🟢	🔴	🟢	🟡	🟢	🟢	🟢
	E' possibile chiedere informazioni se è stato effettuato il vaccino?	🟡	🔴	🔴	🟢	🟡	🔴	🟡	🔴	🔴	🟡	🟢	🟢	🟢	🟢
	E' possibile richiedere alle persone di vaccinarsi?	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴
	Si possono escludere dal luogo di lavoro o dallo svolgimento del proprio ruolo soggetti che non si sono vaccinati?	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴
Visitatori	Si può chiedere ai visitatori informazioni sui sintomi COVID?	🔴	🟡	🔴	🟢	🔴	🔴	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟢
	Si può prendere la lettura della temperatura?	🟡	🔴	🟡	🔴	🔴	🔴	🟡	🟡	🟡	🟡	🟢	🟡	🟡	🟢
	E' possibile richiedere ai visitatori notifiche circa una loro diagnosi positiva?	🟡	🟡	🔴	🟢	🟡	🔴	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢
	E' possibile chiedere ai visitatori informazioni se è stato effettuato il vaccino?	🔴	🔴	🔴	🟢	🟡	🔴	🔴	🔴	🟡	🟡	🟡	🔴	🟢	🟢
	E' possibile escludere dal proprio posto di lavoro visitatori non vaccinati?	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🟡	🔴	🟡	🔴	🟡	🟡
In Generale	Si può registrare chi è infetto?	🟡	🟢	🟡	🟢	🟡	🟡	🔴	🟢	🔴	🔴	🟢	🟢	🟢	🟢
	Si può notificare gli altri dipendenti sulle infezioni?	🔴	🟡	🟢	🟢	🟢	🟡	🟡	🟢	🔴	🟢	🟢	🟢	🟢	🟢
	Si puòavvisare le autorità sanitarie pubbliche?	🟢	🟢	🟢	🟢	🔴	🟢	🟢	🟢	🔴	🟢	🟢	🟢	🟢	🟢
	Legenda														
	SI 🟢														
	SI, ma con limitazioni 🟡														
	NO 🔴														

Tabelle nel File di Lavoro "*excel*" riportato di seguito:

BB summary Ita .xlsx

8. Riflessioni sul nuovo protocollo condiviso di aggiornamento delle misure per il contrasto ed il contenimento della diffusione del virus SARS-COV-2/COVID-19 negli ambienti di lavoro

L'aggiornamento del P*rotocollo condiviso di regolamentazione delle misure per il contrasto ed il contenimento della diffusione del virus COVID-19 negli ambienti di lavoro*, in coerenza con la previsione dell'art. 29 bis della legge n. 40/2020 – che individua nelle previsioni del Protocollo il contenuto concreto dell'art. 2087 del codice civile – risultava necessario per la finalità di acquisire nel documento le novità normative e scientifiche (previsioni di legge, circolari esplicative, evoluzioni delle conoscenze in relazione alle varianti), e quindi attualizzare le regole di sicurezza contro l'epidemia e semplificarne l'applicazione per le imprese. L'adozione di misure di sicurezza stringenti consegue soprattutto alla presenza di varianti, la cui virulenza acuisce il rischio di contagio o in alcune ipotesi appare limitare l'efficacia dei vaccini. L'uso della mascherina riduce il rischio dei contagi e dell'attivazione del "*contact tracing*" e quindi l'adozione di misure di quarantena. Tale uso riduce le ipotesi di diffusione del virus al di fuori dei luoghi di lavoro e nella società, limitando anche l'ipotesi di isolamento e quarantena che riflettono i loro effetti anche sul lavoro. Dall'analisi del testo, si evidenzia che l'impostazione e la struttura del Protocollo non risultano cambiati.

In premessa, si conferma che il COVID-19 "rappresenta un rischio biologico generico, per il quale occorre adottare misure uguali per tutta la popolazione. Il presente Protocollo contiene, quindi, misure che seguono la logica della precauzione e seguono ed attuano le prescrizioni del legislatore e le indicazioni dell'Autorità sanitaria".

Per quanto riguarda l'aggiornamento del Protocollo si confermano le misure per contrastare il diffondersi del virus, dalle mascherine al distanziamento fino alla sanificazione periodica. Nel testo si raccomanda "il massimo utilizzo ove possibile, della modalità di lavoro agile o da remoto" – ovvero il cosiddetto smart working – da parte dei datori di lavoro. Si raccomanda inoltre per le attività produttive che siano limitati al massimo gli spostamenti all'interno dei siti e contingentato l'accesso agli spazi comuni. Tra i punti aggiunti, risulta quello della riammissione al lavoro dopo l'infezione che "avverrà secondo le modalità previste dalla normativa vigente[39]. I lavoratori positivi oltre il ventunesimo giorno saranno riammessi al lavoro solo dopo la negativizzazione del tampone molecolare antigenico effettuato in struttura accreditata o autorizzata dal servizio sanitario". Confermato il principio secondo cui la mancata attuazione del Protocollo determina la sospensione dell'attività fino al ripristino delle condizioni di sicurezza. Inoltre, giacché neppure la vaccinazione

[39] Circolare del ministero della salute del 12 ottobre 2020 ed eventuali successive istruzioni

comporta l'abbandono degli strumenti precauzionali (distanziamento, mascherina, igiene), ciò conferma l'esigenza di un rispetto nell' uso di tali strumenti: corretto diffuso e costante negli ambienti di vita e di lavoro. L'uso della mascherina resta, escluso, nelle situazioni di isolamento delle persone, quindi negli uffici occupati da un solo lavoratore o quando il distanziamento è tale da assicurare l'isolamento come già previsto all'art. 1, comma 2, del DPCM 2 marzo 2021.

Un ulteriore elemento di novità riguarda le trasferte. Scompare il riferimento alla sospensione/annullamento e si indica che "è opportuno che il datore di lavoro, in collaborazione con il medico competente ed il Responsabile del Servizio di Prevenzione e Protezione (RSPP), tenga conto del contesto associato alle diverse tipologie di trasferta previste, anche in riferimento all'andamento epidemiologico delle sedi di destinazione". Tale Protocollo presenta, quindi, elementi di maggior adeguamento alle novità giuridiche ed alle conoscenze scientifiche. Inoltre, pur conservando la natura di percorso autonomo rispetto alla materia di sicurezza sul lavoro è privo di rinvii alla valutazione dei rischi. Ripercorrendo il testo, alla data, non si evidenziano nuovi impatti rispetto al Protocollo precedente in riferimento alla protezione dei dati e tutela della privacy.

9. Uso dei dati di localizzazione e degli strumenti per il tracciamento dei contatti nel contesto dell'emergenza legata al COVID-19 e rapporto di lavoro

Premesso che le tecnologie ed i dati utilizzati per contribuire alla lotta al COVID-19 devono servire a dare maggiori strumenti alle persone, piuttosto che a controllarle e reprimerne i comportamenti, i principi di efficacia, necessità e proporzionalità devono guidare qualsiasi misura adottata dagli Stati membri o dalle istituzioni della Unione Europea che comporti il trattamento di dati personali per combattere il CCOVID-19.

La recente normativa[40] in tema di contrasto all' epidemia da COVID-19 ha istituito il sistema nazionale di tracciamento digitale dei contatti all' evidente fine di "allertare le persone che siano entrate in contatto stretto con soggetti risultati positivi e tutelarne la salute attraverso le misure di prevenzione" (Art.26, d.l. n.28/2020). Abbandonato quindi il *contact tracing* tradizionale che rimesso alle interviste del personale sanitario, sconta la debolezza di essere basato sulla memoria del paziente e sulla sua capacità di indicare soggetti determinati, il *contact tracing* tecnologico consente, attraverso un sistema di intelligenza artificiale, di individuare gli spostamenti ed i luoghi frequentati dai contagiati e, in tal modo, di risalire alle persone che con questi ultimi abbiano avuto contatti. Il Gruppo di supporto digitale della Presidenza del Consiglio dei ministri per l' attuazione delle misure di

[40] Il *contact tracing* tecnologico è disciplinato dall'art. 6 (rubricato *Sistema di allerta Covid-19*) del d.l.n. 28/202, convertito dalla l. n. 70/2020 (entrata in vigore il 30 giugno 2020)

contrasto all' emergenza Covid-19 e la *task force* per la gestione dell'emergenza nominata dal Ministro per l' innovazione tecnologica hanno scelto l' App, denominata Immuni, della società *Bending Spoons*, basata sul programma DP-3T (*Decentralized Privacy - Preserving Proximity Tracing)*, installata su un sistema decentrato che memorizza le informazioni all' interno del singolo dispositivo, nel rispetto del concetto privacy by design, ponendo la privacy dell' utente al centro sin dalla fase della sua progettazione. L' applicazione è basata su una minimizzazione di tutti i dati personali e particolari fino all' eventuale e futuro contatto con l'operatore. Non sono previsti dati di geolocalizzazione essendo sufficiente allo scopo il contatto di prossimità con i terzi soggetti attraverso la memorizzazione del BT_ID (*Bluetooth identification*), in particolare i dati inerenti allo stato di salute vengono memorizzati ed elaborati esclusivamente in locale sul dispositivo dell'utente e non vengono associati ad un'identità o dati anagrafici. Attraverso questo sistema, su piattaforma unica nazionale, basato per l'appunto sull' applicazione Immuni, installata liberamente e volontariamente dagli interessati, sui dispositivi personali di telefonia mobile, gli utenti vengono avvisati tempestivamente di essere entrati in contatto con un soggetto risultato positivo al Covid-19 e vengono loro fornite indicazioni sul comportamento da tenere.

L' Autorità Garante per la protezione dei dati personali con provvedimento n. 95 del 1° giugno 2020 ha autorizzato il Ministero della Salute ad avviare il trattamento relativo al sistema di allerta COVID-19. Sulla base della valutazione di impatto, il trattamento di dati personali effettuato nell' ambito del Sistema viene considerato dal Garante proporzionato, essendo state previste misure volte a garantire il rispetto dei diritti e le libertà degli interessati, attenuando così i rischi che potrebbero derivare dal trattamento. L' Autorità ha chiesto che gli utenti siano informati adeguatamente in ordine al funzionamento dell'algoritmo di calcolo utilizzato per la valutazione del rischio di esposizione al contagio. Essi dovranno essere portati a conoscenza che il sistema potrebbe generare notifiche che non sempre riflettono un'effettiva condizione di rischio. Inoltre, gli utenti dovranno avere la possibilità di disattivare temporaneamente l'applicazione attraverso una funzione facilmente accessibile nella schermata principale. I dati raccolti non potranno essere trattati per finalità non previste dalla norma che istituisce l'applicazione e dovrà essere garantita la trasparenza del trattamento ai fini statistico-epidemiologici. Il tracciamento delle operazioni compiute dagli amministratori di sistema sui sistemi operativi, sulla rete e sulle basi dati dovrà essere assicurato. Infine, per i rischi derivanti da falsi positivi occorrerà adottare misure tecniche ed organizzative e la conservazione degli indirizzi IP dei cellulari dovrà essere allineata ai tempi di rilevamento di anomalie e attacchi. Come precisato poi dal Garante, si evidenza che il trattamento di dati personali raccolti attraverso l'applicazione da parte di soggetti non autorizzati, può determinare un trattamento illecito di dati personali anche penale.

In riferimento all'istituto del consenso, facendo riferimento al principio enunciato dal considerando 52, sancito dall' articolo 9 GDPR, il divieto generale di trattare dati personali relativi allo stato di salute di una persona fisica, considerando le deroghe ad esso , in particolare , quella prevista dall' art.9.2, in questo caso infatti si ha la necessità di tutelare l' interesse vitale dell' interessato o di un'altra persona fisica (lett. c) ovvero motivi di interesse pubblico (lett. g) o di diagnosi, terapia e assistenza sanitaria (lett. h) o dall' interesse pubblico nel settore della sanità pubblica (lett. i), pertanto come esplicitato nel considerando 54 del GDPR, in alcune eccezionali ipotesi è consentito quindi derogare ed il trattamento dei dati personali può essere effettuato anche in assenza del consenso dell' interessato.

Il tracciamento tecnologico dei contagi determina una limitazione della sfera personale "non palpabile nell'immediato, ma molto pervasiva, potenzialmente consentendo il monitoraggio, da parte delle multinazionali digitali (compagnie telefoniche e/o social networks, delle nostre azioni e di tutto quel che riguarda la nostra persona, che rientra nel concetto di "diritto di protezione dei dati personali"[41]. Esso si inserisce tra le nuove frontiere e sfide per la protezione dei dati personali provocate dall' evoluzione tecnologica.

Il *contact tracing* tecnologico produce una compressione del diritto alla protezione dei dati personali, la quale induce ad interrogarsi in ordine alla sua legittimità. Fondamentale chiedersi se tale compressione, giustificata dalla finalità di tutela della salute collettiva ovvero, secondo alcuni, dalla prevalenza accordata alla libertà di iniziativa economica riconosciuta dall' art.41 della Costituzione, sia necessaria per il contenimento della diffusione del virus, e sia proporzionata rispetto alla finalità di tutela della salute collettiva ed alle esigenze di contrasto dell' epidemia, temporanea, limitata al periodo ritenuto sufficiente per scongiurare il pericolo del contagio ai fini di contrasto alla pandemia da Covid-19 in atto. In ogni caso nel rispetto del principio di proporzionalità, a garanzia della legittimità della compressione del diritto al trattamento dei dati personali a tutela della salute pubblica, la Commissione EU e l'EPDB hanno univocamente indirizzato gli Stati membri verso la scelta di una applicazione non obbligatoria.

Nella gestione del rischio nella pandemia da Covid-19, il principio di precauzione, unitamente al principio di proporzionalità, nel bilanciamento tra la tutela della salute e la protezione dei dati personali, ha determinato la tutela della salute quale prevalente comprimendo la protezione dei dati personali che ha trovato espressione in una disciplina semplificata, con la previsione normativa della circolazione dei dati personali e di requisiti di informativa semplificata, al fine di rendere la sorveglianza epidemiologica più efficace e capillare.

[41] D'ARCANGELO L., *Contact tracing e protezione dei dati nella fase 2 dell'epidemia da COVID-19 (anche nel rapporto di lavoro),* in *Giustiziacivile.com, n. 3 (speciale),* p. 6

Il considerando 30 del GDPR precisa come la persona fisica possa essere identificata "le persone fisiche possono essere associate a identificativi *online* prodotti dai dispositivi, dalle apparecchiature, dagli strumenti e dai protocolli utilizzati, quali gli indirizzi IP, i marcatori temporanei (*cookies*) o identificativi di altro tipo, quali i *tag* di identificazione a radiofrequenza. Tali identificativi possono lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai *server*, possono essere utilizzate per creare profili delle persone fisiche e identificarle".

Usando Immuni, allorché un utente informa l'applicazione di essere risultato positivo al test, agli utenti che siano stati in contatto viene inviato automaticamente un messaggio di *alert* sul dispositivo personale con il quale gli viene comunicato di essere stato in contatto, negli ultimi 16 giorni, con una persona risultata positiva, senza che gli sia comunicata l'identità di quest' ultima. Il tutto avviene attraverso identificativi temporanei anonimizzati, senza cioè la possibilità di ricollegare le informazioni di una persona fisica identificata o identificabile. Infatti, Immuni è stata progettata in modo da non aver accesso ai dati di geolocalizzazione, non consentendo di tracciare la posizione dei singoli utenti, ma, limitandosi a fornire solo informazioni di prossimità.

Complesse sono le considerazioni che il *contact tracing* pone qualora il tracciamento venga effettuato all' interno del rapporto di lavoro. In tal caso è necessario armonizzare la disciplina speciale relativa al rapporto di lavoro subordinato ed il bilanciamento tra i diversi interessi in gioco quali tutela della salute pubblica, protezione dati personali e tutela della dignità del lavoratore anche in base al principio di non discriminazione.

Sul luogo di lavoro il tracciamento digitale dei contatti attraverso Immuni costituisce una forma di controllo a distanza dei lavoratori attuata attraverso *wearable device*. Queste forme di controllo a distanza, vietate dall' arti.4, comma 1, Statuto dei lavoratori, rientrano, accanto agli impianti di videosorveglianza e agli strumenti di lavoro, tra gli altri strumenti che, secondo la normativa vigente, possono essere impiegati, previa mediazione sindacale e/o amministrativa, per finalità di "sicurezza del lavoro". Occorre pertanto contemperare il diritto del datore di lavoro, alla libertà di iniziativa economica, art. 41 della Costituzione, con il principio personalistico "che pone in primo piano, nella sfera dell' essere, la personalità del lavoratore, rispetto all' iniziativa economica, nella sfera dell' avere" [42], e ai fini della tutela della dignità del lavoratore, l' art.4, comma 1, Statuto dei lavoratori, che ne vieta il controllo a distanza attuato anche attraverso le nuove tecnologie, indipendentemente da quando tale controllo sia effettuato, se durante lo svolgimento dell' attività lavorativa o al di fuori.

[42] CASILLO R., *La dignità nel rapporto di lavoro, in RDC*, n. 5, 2008, p.593

CAPITOLO III
SMART WORKING: CONCILIARE, INNOVARE E COMPETERE UNO STRUMENTO PER LA GESTIONE DELL' EMERGENZA

1. Smart Working: fondamenti ed istruzioni

La diffusione del nuovo Coronavirus (SARS-CoV-2) e la conseguente emergenza epidemiologica hanno dato nuovi impulsi ai processi di modernizzazione della economia e della società in atto da tempo. In questo nuovo ordine economico e sociale un caso emblematico è sicuramente rappresentato dal lavoro agile o *smart working* che ha spinto alcuni a parlare di "nuova normalità".

"Nell'ambito delle misure adottate dal Governo per il contenimento e la gestione dell'emergenza epidemiologica da ***COVID-19 (coronavirus)****, il Presidente del Consiglio dei ministri ha emanato il 1° marzo 2020 un nuovo Decreto che interviene anche sulle modalità di accesso allo smart working. Conciliare, innovare e competere. Sono questi i tre diversi obiettivi smart working, come spiegato sul sito del Governo. Modalità di lavoro che si configura come un nuovo approccio all'organizzazione aziendale, in cui le esigenze individuali del lavoratore si contemperano, in maniera complementare, con quelle dell'impresa"*[43].

In effetti dopo una cauta sperimentazione, seguita dalla pubblicazione in Gazzetta Ufficiale della legge n.81/2017, questa nuova organizzazione del lavoro[44] si è imposta quale strumento principe per conciliare la tutela della salute dei lavoratori con l'esigenza di non fermare l'economia nazionale. L' accelerazione di questa applicazione dello smart working, repentina e generalizzata, ha portato alla formazione di due schieramenti contrapposti, da un lato chi si è espresso apertamente a favore di questa innovazione, capace di garantire produttività per le imprese e benessere per i lavoratori, dall'altro chi invece dal ricorso senza consapevolezza e preparazione a tale strumento ha manifestato riserve e preoccupazioni sul medio e lungo periodo. Tali contrapposizioni non sono nuove agli studiosi dell'evoluzione del lavoro, della sua concezione nell' economia e nella società e delle sue regole giuridiche.

Lo *smart working*[45], come innovazione incide sui tempi di vita e di lavoro e sul nodo produttività, collegato come è alla digitalizzazione del lavoro e alle nuove tecnologie. Non possiamo non far riferimento alle battaglie sindacali del Novecento industriale o ad altre rivoluzioni del recente passato, legate al lavoro a tempo parziale, che ha spinto la femminilizzazione del mercato del lavoro, e nel

[43] http://www.sitiarcheologici.palazzochigi.it/www.governo.it/febbraio%202021/node/14210.html
[44] PESSI R., *Lezioni di diritto del lavoro*, Giappichelli Editore 2018, pag. 377-378
[45] PESSI R., Op. Cit.

tempo, ha dimostrato limiti e criticità rispetto al nodo della libertà della determinazione del tempo di lavoro e della contrapposizione tra lavoro produttivo e lavoro familiare. Posto che in particolare il lavoro a tempo parziale cercava di tenere separati il tempo dedicato al lavoro e il tempo dedicato ai carichi familiari, lo smart working relativizzando il concetto di orario di lavoro promuove logiche di lavoro per obiettivi. Lavorare per obiettivi, cioè in funzione dei risultati piuttosto che dello scorrere del tempo ha chiaro riferimento nella norma di apertura della disciplina giuridica del lavoro agile, art. 18 della legge n.81/2017 che si esprime in termini di forme di organizzazione del lavoro "per fasi, cicli e obiettivi e senza precisi vincoli di orario o luogo di lavoro". Il legislatore inserisce lo smart working dentro la omnicomprensiva categoria della subordinazione giuridica, art.18, comma 1, legge n.81/2017 scaricando automaticamente le relative responsabilità di utilizzo della prestazione sul datore di lavoro, pur perdendone il controllo e l'organizzazione della prestazione di lavoro stessa.

La sfida dello *smart working* non sta nel ripensare tanto e solo logiche manageriali di gestione del personale[46] quanto la stessa struttura dell'attuale sistema economico del lavoro dipendente, il mercato e l'impresa senza trascurare le esternalità economiche e l'impatto sul sistema sociale. La pandemia non ha solo posto al centro le questioni inerenti ai livelli occupazionali ma ha riacceso con dirompenza lo strumento del lavoro da remoto. Se infatti pochi mesi prima dall' inizio dell'emergenza il nostro smart working era considerato una forma di welfare volto alla conciliazione vita-lavoro, adottato in sparuti casi, ora è posto al centro della discussione sugli elementi strutturali del lavoro del futuro.

Non è banale notare che di *smart working* e di lavoro agile, si parla solo in Italia, infatti anche nei paesi di lingua anglosassone, che anticipano le trasformazioni del lavoro, si parla di lavoro da remoto o telelavoro. Il legislatore italiano ha scelto la formula espressiva di "lavoro agile" (art. 18, comma1, l. n.81/2017) cercando così di differenziarlo in chiave normativa (fattispecie ed effetti) dal "telelavoro" regolato dall' accordo – quadro europeo 16 luglio 2002 tra Unice/Ueapme, Ceep e Ces (recepito in Italia con l'accordo interconfederale del 9 giugno 2004). In realtà durante la pandemia, indipendentemente dalla terminologia rassicurante adottata dal Governo nell' accompagnare l'emergenza sanitaria da Covid-19, si è realizzato un faticoso esercizio di "lavoro domiciliare forzato"[47], almeno con riferimento a quel gruppo più fortunato di lavoratori impegnati in servizi, settori e prestazioni essenziali che hanno potuto proseguire in modalità da remoto.
L' attuale legislazione non si è fatta carico di sciogliere tutti i nodi che solleva il lavoro reso da remoto (seppur alternato a lavoro in presenza) lasciando ampio spazio a una contrattazione collettiva che sta procedendo senza linee guida uniformi a livello nazionale col rischio di incidere significativamente nelle dinamiche di concorrenza tra imprese dello stesso settore.

[46] BUTERA F. *Le condizioni organizzative e professionali dello smart working dopo l'emergenza: progettare lavoro ubiquo fatto di ruoli aperti e di professioni a banda larga* in Stud. Org., n.1 2020, pp. 141.165
[47] DAGNINO E., MENEGOTTO M., PELUSI M. L., TIRABOSCHI M. *Guida pratica al lavoro agile* ADAPT University Press, 2020 pp. 6

Fondamentale è la previsione di cui all' art.18, comma 1, della l. n.81/2017 che si limita, nel delineare determinati effetti e vincoli all' utilizzo dell'istituto, a tutte quelle prestazioni di lavoro subordinato che siano svolte, almeno in parte, al di fuori dei locali aziendali, pur potendo essere svolte anche all' interno, e senza una postazione fissa, così da cercare di differenziare la fattispecie da altri lavori e, di regola, mediante il ricorso a strumenti telematici ed informatici. Legge 22 maggio 2017, n.81, articolo 18: *"Le disposizioni del presente capo, allo scopo di incrementare la competitività e agevolare la conciliazione dei tempi di vita e lavoro, promuovono il lavoro agile quale modalità di esecuzione del rapporto di lavoro subordinato stabilita mediante accordo tra le parti, anche con forme di organizzazione per fasi, cicli e obiettivi e senza precisi vincoli di orario o di luogo di lavoro, con il possibile utilizzo di strumenti tecnologici per lo svolgimento dell'attività lavorative. La prestazione lavorativa viene eseguita, in parte all' interno di locali aziendali e in parte all' esterno senza una postazione fissa, entro i soli limiti di durata massima dell'orario di lavoro giornaliero e settimanale, derivanti dalla legge dalla contrattazione collettiva".*

Non rientrano in questo contenitore di "lavoro agile", secondo tale definizione legale, tutte quelle forme di lavoro autonomo, che da tempo si sviluppano in funzione di obiettivi e progetti o fasi di lavoro senza precisi vincoli di tempo e luogo della prestazione, posto che il tempo ed il luogo sono indici identificativi del solo lavoro dipendente.

2. Il quadro normativo

Gli aspetti organizzativi e culturali, legati alla specificazione delle finalità e alla messa in atto delle procedure di coinvolgimento e formazione dei lavoratori, unitamente al rispetto dei vincoli di natura giuridica sono alla base dell'attuazione ed implementazione del lavoro agile. Il lavoro agile non si configura come un nuovo contratto di lavoro, bensì come "una modalità di esecuzione del rapporto di lavoro subordinato e dunque come una mera modalità di organizzazione del lavoro". Ai fini dell'attivazione di tale modalità risulta necessaria un'espressa clausola negoziale, per il tramite della stipulazione di un accordo individuale tra datore di lavoro e lavoratore (art.18, comma1 l.n.81/2017), posto che dopo l'emergenza sanitaria da Covid-19, il legislatore ha temporaneamente sospeso tale requisito, al fine di gestire una situazione epidemiologica di enorme gravità. L'adesione al lavoro agile ha natura consensuale e volontaria, e non è richiesta la stipulazione di un accordo collettivo o di una policy aziendale. L'accordo individuale si configura come condizione necessaria e sufficiente per un'attivazione del lavoro agile in conformità ai vincoli di legge.

L' art.19, comma 1, della l. n.81/2017 dispone che "l'accordo relativo alla modalità di lavoro agile è stipulato per iscritto ai fini della regolarità amministrativa e della prova". L' accordo sulla modalità

di lavoro agile, al pari delle sue eventuali modificazioni, rientra tra gli atti da comunicare in via obbligatoria al centro per l'impiego competente per territorio entro il giorno antecedente l'inizio della prestazione secondo tale modalità. Tanto l'inosservanza quanto il mero ritardo nell' adempimento di tali obblighi di comunicazione sono sanzionati in via amministrativa.

Se nessun profilo di incompatibilità si pone rispetto agli ordinari rapporti di lavoro a tempo pieno (sia a tempo determinato che indeterminato), particolari considerazioni ricadono sul contratto di apprendistato, i contratti di lavoro part-time, il contratto di lavoro intermittente nonché la somministrazione di lavoro. Un caso particolare è quello del tirocinio formativo e di orientamento, che non essendo un contratto di lavoro non rientra nell'ambito della l. 81/2017, sebbene nella prassi, dopo l'emergenza sanitaria da Covid-19, anche in riferimento a questo istituto si parli di "lavoro agile". Per il contratto di apprendistato, la sua disciplina non prescrivendo affiancamento fisico o costante e permanente, se gli obblighi formativi e di affiancamento possono esser gestiti in modalità virtuale, non si pongono problemi per l'utilizzabilità di tale modalità di lavoro.

Quanto al contratto di lavoro part-time, un profilo di potenziale incompatibilità potrebbe essere riscontrato dall' obbligo di specificare all' interno del contratto di lavoro la collocazione temporale e la durata della prestazione, poco coerente con la flessibilità del lavoro agile. Tuttavia, la puntuale collocazione della prestazione lavorativa è una tutela per il lavoratore.

Quanto alla somministrazione di lavoro, in ragione della dissociazione che si verifica tra il datore di lavoro formale (agenzia) e l'effettivo utilizzatore della prestazione lavorativa, si pone una complessità non banale nel definire la compatibilità col lavoro agile. Posto che l'accordo di lavoro agile dovrà essere stipulato dall' agenzia, datore di lavoro formale, ma la sua attuazione dipende dalla volontà dell'utilizzatore, quindi risulta ragionevole, anzi necessaria, la stipula di un accordo tra tutte le parti del contratto.

Premesso che è in capo al datore di lavoro il potere di individuare i soggetti con i quali concordare la modalità di lavoro agile, a parte i profili di compatibilità, risulta rilevante individuare i criteri di accesso ed i potenziali destinatari del lavoro agile all' interno di policy aziendali o di accordi collettivi, evitando contenziosi e tensioni.

Sebbene la disciplina emergenziale abbia introdotto per alcune categorie di lavoratori, un vero e proprio diritto a svolgere la prestazione in modalità di lavoro agile alla luce di requisiti soggettivi e oggettivi, la disciplina ordinaria del lavoro agile non prevede l'esistenza di un tale diritto. La previsione, contenuta nella l. 81/2017 ha introdotto un diritto di priorità, ampliato poi dalla disciplina emergenziale e alla riconducibilità della adibizione a lavoro agile nell'ambito delle misure di accomodamento ragionevole ai sensi della convenzione ONU sui diritti delle persone con disabilità del 13 dicembre 2006. Secondo l'art.18, comma 3-bis, della l.81/2017 occorre riconoscere la priorità

per l'accesso al lavoro agile "alle lavoratrici nei tre anni successivi alla conclusone del periodo di congedo di maternità" e "ai lavoratori con figli in condizioni di disabilità ai sensi dell'articolo 3, comma 3, della legge 5 febbraio 1992, n.104". A tale previsione si aggiunge, ai sensi dell'art.39, commi2 2-bis, d.l.n.18/2020 la priorità delle richieste per "i lavoratori del settore privato affetti da gravi e comprovate patologie con ridotta capacità lavorativa" o "i lavoratori immunodepressi e ai familiari conviventi di persone immunodepresse". Quindi lavoro agile inteso quale accomodamento ragionevole al fine di garantire la parità di trattamento dei lavoratori affetti da disabilità.

Quanto alla disciplina relativa alla esecuzione della prestazione svolta fuori dall' ufficio o dai locali aziendali, resta in capo all' interprete individuare quali siano i contenuti da inserire nell' accordo ai fini della disciplina della prestazione resa all' esterno dei locali aziendali. Quanto al luogo di lavoro, la legge prevede che il lavoro agile sia svolto, con riferimento alla prestazione esterna all' ufficio o ai locali aziendali, senza la presenza di una sede fissa. Disciplina delle modalità di esecuzione esterna della prestazione, inclusi potere direttivo e i relativi strumenti di lavoro risultano essere contenuti necessari dell'accordo (art.19, comma1, della l. n.81/2017).

Nell' accordo individuale di lavoro agile, come da previsione del comma 1 dell'art. 19, secondo periodo, occorre individuare "i tempi di riposo del lavoratore nonché da misure tecniche ed organizzative necessaria per assicurare la disconnessione del lavoratore dalle strumentazioni tecnologiche di lavoro". Disposizioni che mirano a tutelare il lavoratore dai rischi di *overworking* così come da quelli derivanti dall' assenza di una netta separazione tra vita lavorativa e vita privata. Si tratta di un fenomeno emerso con evidenza nel corso dell'emergenza sanitaria Covid-19 e sicuramente emblematico all' interno della trasformazione tecnologica di questi ultimi anni. A parte i profili descrittivi e prescrittivi della definizione in materia di orario di lavoro, con riferimento ai limiti massimi ed alle deroghe, l'interpretazione prudenziale tende ad assicurare quanto meno il rispetto delle undici ore consecutive di riposo. L' applicazione delle deroghe alla disciplina di orario di lavoro dipendono da autonomia organizzativa riconosciuta al dipendente. Quanto al diritto alla disconnessione il legislatore italiano rimanda alle parti più vicine al rapporto (l'accordo tra lavoratore e datore di lavoro, mediato dall' azione sindacale) le modalità tecniche ed organizzative di attuazione. L' esercizio del potere di controllo rappresenta un ulteriore contenuto necessario dell'accordo individuale. Infatti, ai sensi dell'art.21 della l.n.81/2017 l'accordo di lavoro agile "disciplina l'esercizio del potere di controllo del datore di lavoro sulla prestazione resa dal lavoratore all' esterno dei locali aziendali nel rispetto di quanto disposto dall' art.4 della l. 20 maggio 1970 n.300 e successive modificazioni". Sebbene come commentato da Pietro Ichino non pare nulla aggiungere in merito al necessario rispetto della disciplina in materia di controlli a distanza e di quella del codice della privacy. L'accordo potrà limitarsi a confermare la piena applicabilità della previsione statutaria e a specificare il regime di utilizzabilità dei dati (ai sensi dell'art.4, comma3), richiamando

l'informativa relativa alle modalità d' uso degli strumenti e di effettuazione dei controlli. La gestione al fine dell'utilizzabilità dei dati richiederà, ai sensi del comma3 dell'art.4 novellato, una grande attenzione nella predisposizione di disciplinari d' uso e di informative sulle modalità di controllo, policy aziendali risultano fortemente consigliate. Profili di incertezza permangono sulla modalità applicativa di eventuali controlli, con riferimento alla pratica BYOD (*Bring your own device*). In riferimento all' esercizio di potere disciplinare, l'art.21 della l. n. 81/2017, si preoccupa al comma 2, di regolare alcuni profili relativi all' esercizio del potere disciplinare da parte del datore di lavoro. L' accordo di lavoro agile occorre che individui "le condotte, connesse all' esecuzione della prestazione lavorativa all' esterno dei locali aziendali, che danno luogo all' applicazione di sanzioni disciplinari". Si tratta di una disposizione che va ad a ampliare i poteri del datore di lavoro in questo ambito e/o magari a derogare alcune previsioni in materia.

L'accordo di lavoro agile potrà avere durata a tempo determinato o indeterminato, a prescindere dalla durata a tempo determinato del contratto di lavoro su cui la modalità di lavoro si innesta. Un accordo a termine potrà essere utilizzato, a fini di reciproca sperimentazione della modalità di lavoro tra le parti, con riferimento ad un contratto a tempo indeterminato, e non è da escludere la sottoscrizione di un accordo a tempo indeterminato per rapporti di lavoro a termine. La disciplina in materia di recesso è dettata dal comma 2 dell'art. 19 della l. n. 81/2017, distinguendo tra accordo a tempo indeterminato e accordo a tempo determinato. Con riferimento alla prima tipologia di accordo si prevede un regime di libera recedibilità dall' accordo (recesso *ad nutum* dall' accordo, non dal contratto di lavoro sottostante), ma nel rispetto di termini di preavviso minimi.

In materia di tutela e sicurezza con la l.n. 81/2017 il legislatore si è fatto interprete di un'esigenza di semplificazione e alleggerimento della normativa applicabile al telelavoro, normativa che per una parte di commentatori e del mondo imprenditoriale, configurava un freno notevole alla diffusione del lavoro da remoto. Il legislatore ha quindi approntato su questo piano, un impianto minimalistico, basato sull' art.22 della l. n. 81/2017, cui si aggiunge il comma 2 dell'art.18 con specifico riferimento alla sicurezza delle strumentazioni tecnologiche. Il comma 1 dell'art.22 della l.n.81/2017 sancisce il principio secondo il quale il datore di lavoro è tenuto a garantire la salute e la sicurezza del lavoratore che svolge la prestazione in modalità di lavoro agile. Nello stesso comma 1 viene ulteriormente specificato che almeno una volta l'anno il datore di lavoro debba consegnare al lavoratore e al rappresentante dei lavoratori per la sicurezza un'informativa scritta nella quale sono individuati i rischi generali e specifici. A livello comunitario la materia è regolata dalla direttiva quadro 89/391/CEE (attuazione di misure volte a promuovere il miglioramento della sicurezza e della salute) e dalla direttiva 90/270/CE (prescrizioni minime in materia di sicurezza e salute per le attività lavorative svolte su attrezzature munite di videoterminali). A garanzia delle stesse imprese, a fronte di dati inequivocabili, volta a fornire una ricostruzione della disciplina di salute e sicurezza del lavoro

agile è data dall'art.3, comma 10, del dlgs.n.81/2008 che racchiude difatti la disciplina prevenzionistica "relativa ai lavoratori subordinati che effettuano una prestazione continuativa di lavoro a distanza, mediante collegamento informatico e telematico", con riferimento tanto ai lavoratori pubblici che privati. Tanto il dlgs.n.81/2008 quanto la l.n.81/2017 prevedono a carico del lavoratore un obbligo di cooperazione rispetto all'attuazione delle misure di prevenzione adottate dal datore. Il lavoratore dovrà quindi optare per un luogo esterno di lavoro che gli consenta il pieno esercizio della propria attività lavorativa in ossequio alle normative sulla sicurezza, secondo quanto appreso durante appositi corsi di formazione.

Per completezza del quadro normativo l'art.23 l.n.81/2017 estende la copertura assicurativa alle prestazioni di lavoro agile rese all'esterno della sede aziendale e lontano dalla sfera di controllo del datore. L'estensione della copertura riguarda tanto l'infortunio che avvenga durante la prestazione di lavoro agile quanto l'infortunio in itinere. La normativa italiana del lavoro agile prevede infine alcuni ulteriori aspetti di disciplina di particolare rilevanza ai fini di una corretta gestione della modalità di lavoro agile. L'art.20 comma 1, statuisce che "il lavoratore che svolge la prestazione in modalità di lavoro agile ha diritto ad un trattamento economico e normativo non inferiore a quello complessivamente applicato, in attuazione dei contratti collettivi di cui all'art.51 del decreto legislativo 15 giugno 2015, n.81, nei confronti dei lavoratori che svolgono le medesime mansioni esclusivamente all'interno dell'azienda". La parità di trattamento nei confronti dei lavoratori agili viene parametrata al trattamento economico e normativo applicato a soggetti che svolgano le stesse mansioni esclusivamente all'interno dei locali aziendali. I contratti collettivi nazionali, territoriali o aziendali utilizzati per parametrare sono quelli stipulati dalle associazioni sindacali più rappresentative sul piano nazionale.

3. Smart Working ed emergenza pandemica

Tra gli strumenti diretti ad arginare la diffusione e gli effetti economici negativi, generati dall' emergenza pandemica, il Governo si è da subito orientato sull' utilizzo della modalità di lavoro agile. A partire dal 23 febbraio 2020, il Governo ha prodotto e replicato discipline emergenziali volte ad agevolare l'adozione del lavoro agile, anche attraverso deroghe e semplificazioni alla disciplina vigente, per garantire il necessario distanziamento sociale nei contesti lavorativi e per diminuire al minimo le occasioni di contatto interpersonale. Un'attenzione particolare si è aggiunta, in un momento successivo all' intervento di semplificazione, rispetto alla definizione di specifiche ipotesi e categorie di lavoratori cui riconoscere un diritto o una priorità all' adibizione al lavoro agile, a tutela di soggetti particolarmente vulnerabili e per rispondere alle esigenze di cura cui i lavoratori si sono trovati a far fronte.

Dopo una reiterazione all' interno di diversi D.P.C.M. adottati a partire da febbraio, la normativa si è consolidata con l'art. 90 del d.l. n.34/2020, convertito dalla l. n. 77/2020, la cui applicazione risulta estesa, grazie al rinvio mobile ivi incluso fino al 31 dicembre.

In estrema sintesi l'intervento normativo ha inteso semplificare l'adozione della modalità di lavoro agile nella fase emergenziale in tre dimensioni: il venir meno della necessità di stipulazione di un accordo individuale di lavoro agile, la possibilità di adempiere in forma semplificata all'obbligo di informativa in materia di salute e sicurezza e la modalità di comunicazione dell'adibizione dei lavoratori nella modalità agile. L' intervento di semplificazione maggiormente incisivo rispetto al massimo utilizzo di lavoro agile è la possibilità di adozione del lavoro agile senza la necessità di previa stipulazione dell'accordo individuale comma 4 dell'art. 90 del d.l. n.34/2020. Tale previsione determina oltre al venir meno dei tempi e dei costi connessi alla stipulazione sul piano individuale di accordi anche il venir meno del principio cardine di volontarietà. Il datore di lavoro, pertanto, può unilateralmente disporre e proporre il lavoro agile, ai fini di garanzia della salute dei propri lavoratori, nell' adempimento del suo obbligo di tutelare la salute e sicurezza del lavoratore, anche in applicazione dei protocolli anti-contagio.
La disposizione in ogni caso prevede il rispetto dei principi della l. n. 81/2017, principi di cui dare riscontro preferibilmente all' interno di una comunicazione ai dipendenti. Dalla norma si pone particolare attenzione ai seguenti aspetti:

- Esercizio dei poteri datoriali, da esercitare nei limiti di legge, in particolar riguardo per il tramite di strumenti digitali
- Tempo di lavoro e disconnessione, nel rispetto dei limiti massimi previsti
- Luogo di lavoro, considerato l'obiettivo della tutela della salute dei lavoratori, risulta preferibile l'esclusione di luoghi pubblici o aperti al pubblico e considerare la possibilità di lavoro dal domicilio o da latro luogo di pertinenza del lavoratore
- Strumenti di lavoro, non esiste un vincolo di consegna degli strumenti di lavoro e quindi i lavoratori potranno usare anche il PC personale (rif. comma 2 dell'art.90 del d.l.n. 34/2020)

Si osserva inoltre che la predisposizione di una minima scheda informativa o lettera unilaterale di adibizione, riguardante le materie citate, rappresenti un utile strumento a tutela delle parti.
Il Governo ha inoltre introdotto semplificazioni rispetto all'obbligo di informativa in materia di salute e sicurezza (rif. comma 3 dell'art.90 del d.l.n. 34/2020), che può avvenire in via telematica e per il tramite di un modello standard fornito dall' INAIL. Trattasi di un'agevolazione che consente alle aziende di tagliare tempi necessari per l'adibizione al lavoro agile e costi relativi ad un'attività di solito basata su consulenza specialistica.

Rispetto ai diritti e le priorità il quadro di riferimento consta in un insieme di disposizioni disseminate in diversi atti normativi, con termini temporali applicativi differenti. Alcune disposizioni hanno peraltro cessato i propri effetti, basti pensare al diritto al lavoro agile per genitori con figli under 14 anni (art. 90, comma1, del d.l. n.34/2020), la ratio è difatti decaduta con la riapertura delle scuole. In ogni caso gli interventi in materia di introduzione di diritti e priorità al lavoro agile si possono distinguere in interventi a tutela di soggetti vulnerabili ed in risposta ad aumentate esigenze di cura. Per la tutela dei soggetti vulnerabili occorre far riferimento alle disposizioni di cui all' art.30 del d.l.n.18/2020.Con esse si introduce il diritto al lavoro agile per lavoratori disabili o che "abbiano nel proprio nucleo familiare una persona con disabilità nelle condizioni di cui all' art. 3, comma 3, della legge 5 febbraio 1992, n.104", esteso ai sensi del comma 2 " ai lavoratori e ai familiari di persone immunodepresse" sempre che l' attività lavorativa sia compatibile col suo svolgimento da remoto. Si riconosce inoltre priorità nell' accoglimento di richieste di lavoro agile da parte di lavoratori affetti da gravi patologie con ridotta capacità lavorativa e per lavoratori immunodepressi o loro familiari. Inoltre, grazie all' art.90 comma 1, del d.l.n.34/2020 si sancisce il diritto al lavoro agile, sempre con prestazione compatibile da remoto, sulla base della valutazione del medico competente "in ragione dell'età o della condizione di rischio derivante da immunodepressione, da esiti di patologie oncologiche o dallo svolgimento di patologie oncologiche o terapie salvavita da comorbilità che possono caratterizzare una situazione di maggiore rischiosità (…)".

L' art. 26 del d.l.n. 18/2020, comma 2-bis, prevede che i lavoratori fragili " lavoratori dipendenti pubblici o privati in possesso di certificazione rilasciata da competenti organi medico-legali, attestante una condizione di rischio derivante da immunodepressione o da esiti di patologie oncologiche o dallo svolgimento di terapie salvavita ivi inclusi i lavoratori in possesso del riconoscimento di disabilità con connotazione di gravità- possano svolgere la prestazione in lavoro agile " anche attraverso adibizione a diversa mansione, ricompresa nella medesima categoria o area di inquadramento come definite dai contratti collettivi vigenti.

4. Emergenza Covid-19 e le scelte dei governi in EU e negli USA

In tutti i Paesi colpiti dalla pandemia il lavoro da remoto[48] è stata una scelta obbligata per la prosecuzione delle attività. Al fine di cogliere il peso di questa misura nella gestione dell'emergenza sanitaria è necessario evidenziare la diffusione del lavoro da remoto all'interno dei vari Paesi maggiormente colpiti. Da una prima analisi emerge chiaramente come l'Italia fosse molto indietro nell'implementazione di questa modalità di lavoro rispetto ad altri Paesi. In Italia solo il 7% dei lavoratori aveva accesso alla modalità di lavoro da remoto, di cui l'1% costituito dai telelavoratori e

[48] PIGNI G. *Il lavoro da remoto come misura necessaria per affrontare l'emergenza Covid-19 – Le scelte dei governi in Europa e negli Usa*, WP n. 14, ADAPT University Press 2020

il 5% dagli smart workers, numeri sensibilmente inferiori rispetto agli altri paesi come gli Stati Uniti (37%), Regno Unito (26%), Francia (25%), Spagna (13%), Germania (12%). La pandemia ha stravolto questi dati. Sulla base dei dati raccolti nell'ambito del progetto Repeat (*REpresentations, PErceptions and ATtitudes on the Covid-19*)[49] pur dovendo considerare il diverso impatto della pandemia nei diversi Paesi, emerge che a fine Marzo (2020) in Italia il 35 % dei lavoratori prestava servizio da casa e il 47% aveva smesso di lavorare, in Germania il 24% lavorava da casa ma solo il 23% aveva smesso di lavorare, in Francia il 34% lavorava da casa mentre il 28% aveva smesso di lavorare, nel Regno Unito il 46% lavorava da casa mentre il 32% si era fermato. Oltreoceano il ricorso al lavoro da remoto è sembrato essere in linea con quanto registrato nella fase pre-Covid, anche perché il modello statunitense ha risposto all'emergenza seguendo logiche di politica occupazionale differenti rispetto a quelle europee. Sulla base della seconda rilevazione del progetto Repeat, la percentuale dei lavoratori non attivi in Italia è sembrata diminuire, passando dal 47% al 34%. La riduzione è stata dovuta sia ad un aumento del lavoro da casa che di quello presso il regolare posto di lavoro. Al fine di completare l'analisi svolta dal progetto Repeat è risultato utile quantificare il numero di posti di lavoro potenzialmente prestabiliti da remoto. Tale dato è piuttosto significativo poiché ha mostrato le potenzialità di un mercato del lavoro rispetto al tema del lavoro da remoto, evidenziando la mancanza di volontà nell'investire in questa forma di lavoro. In Spagna, ad esempio si è calcolato che nell'ultimo anno dei 19,8 milioni di persone impiegate, 951000 abbiano svolto telelavoro in metà dei giorni lavorativi e 688.700 lo abbiano fatto occasionalmente. Dati estremamente bassi se confrontati con la stima di 4,4 milioni di posti di lavoro prestabiliti da remoto (il 23% del totale). Negli Stati Uniti invece, se da una parte risultava ordinariamente abbastanza comune svolgere occasionalmente lavoro da casa, dall'altra parte è necessario sottolineare come solo una piccola porzione dei lavoratori abbia avuto la possibilità di lavorare stabilmente da casa (il 7%).

In relazione all'emergenza pandemica la tendenza generale e comune alla maggior parte dei Paesi colpiti dal virus è stata quella di facilitare l'implementazione del lavoro da remoto. L'Italia, primo Paese europeo ad essere colpito in maniera diretta dalla pandemia, ha predisposto una procedura di semplificazione della procedura di attivazione dello *smart working*, rivolta innanzitutto alle "zone rosse" per poi allargarsi alle altre più impattate e arrivando con il DPCM del 1°marzo 2020 a coinvolgere tutto il territorio nazionale. È stata dunque riconosciuta la possibilità per i datori di lavoro privati di ricorrere al lavoro agile (legge n.81 del 22 maggio 2017) senza accordo individuale con il dipendente e assolvendo in modalità telematica e semplificata l'obbligo informativo in materia di salute e sicurezza. Per il settore pubblico invece si è rinviato all'articolo 87 del decreto-legge 18/2020 in base al quale lo *smart working* è divenuto la modalità ordinaria di svolgimento della prestazione

[49] Progetto coordinato da Sylvain Brouard (Sciences Po, CEVIPOF), Michael Becher (IAST, Università di Tolosa 1), Martial Foucault (Sciences Po, CEVIPOF) e Pavlos Vasilopoulos (Università di York e CEVIPOF)

lavorativa nelle pubbliche amministrazioni. L'incentivazione dello smart working si è tradotta nel riconoscimento, in capo al lavoratore, del diritto di poter accedere al lavoro agile, accertata la sussistenza delle condizioni per ricorrerci. Infine, fondamentale considerare la presenza, nelle regioni maggiormente, interessate dal virus di una forma di incentivazione diretta al ricorso a questa forma di lavoro. Ossia forme di agevolazione economiche dirette al finanziamento dei servizi di consulenza e formazione finalizzati sia all'adozione di un piano di *smart working*, sia all'acquisto di strumenti tecnologici funzionali all'attuazione del piano stesso.

La linea italiana è stata seguita anche dal governo spagnolo. In Spagna il lavoro da remoto (o *teletrabajo*), è inserito all'interno della Ley del Estatuto del los Trabajadores (legge dello statuto dei lavoratori) ai sensi dell'articolo 13. Con il regio decreto-legge n.6 del 1°marzo 2019, il lavoro a distanza è stato riconosciuto come una possibilità per i lavoratori di conciliare meglio lavoro e vita privata. Vi è la possibilità di richiedere la modalità *home office* fino a quando i propri figli non abbiano raggiunto i 12 anni di età. In relazione alla gestione dell'emergenza, la Spagna proprio come l'Italia, ha adottato misure volte a facilitare il *teletrabajo*. Innanzitutto, è stato previsto che l'accordo tra le parti del contratto di lavoro a distanza non fosse più richiesto. L'articolo 5 del regio decreto-legge n.8 del 17 marzo 2020 ha tramutato il *teletrabajo* come un'opzione preferenziale per le aziende e i lavoratori. In tema di prevenzione dei rischi per la salute e la sicurezza del lavoro, permettendo al lavoratore di autocertificare il rispetto delle misure di sicurezza.

In Francia il lavoro da remoto (*télétravail*) è definito come qualsiasi forma di organizzazione del lavoro in cui il lavoro che avrebbe potuto essere svolto nei locali del datore di lavoro è svolto dal dipendente al di fuori di tali locali su base volontaria, utilizzando le tecnologie dell'informazione e della comunicazione. Per completezza del quadro normativo, importante citare l'Accordo nazionale interprofessionale (ANI) sul telelavoro del 2005 che ha imposto l'assunzione dei costi relativi al telelavoro da parte dell'azienda e l'obbligo per il datore di lavoro di fornire per iscritto le informazioni relative alle condizioni di esecuzione del lavoro. Al contrario della Spagna e dell'Italia il governo francese non ha dovuto adeguare la normativa riguardante il *télétravail* alle esigenze della crisi pandemica, giacché la stessa L-1222-11 considera, di fronte a circostanze eccezionali, in particolare la minaccia di un'epidemia, o in casi di forza maggiore, l'attuazione del telelavoro come adeguamento della postazione di lavoro reso necessario per consentire la continuità dell'attività aziendale e garantire la tutela dei dipendenti. Il rischio di epidemia si concretizza dunque come giustificazione per l'impostazione del *teletravail* senza il consenso del lavoratore al fine di adempiere all'obbligo di tutela della salute e della sicurezza dei lavoratori in capo al datore di lavoro. Ciò è stato fra l'altro confermato dal Ministero del Lavoro francese, il quale ha precisato nel mese di aprile, che questa forma di eccezionale di telelavoro non richieda alcun tipo di formalismo.

Anche l'ordinamento tedesco come quello francese non registra modifiche normative volte alla valorizzazione del lavoro da remoto. Il Ministero del lavoro non ha riconosciuto alcun diritto legale a lavorare da casa, in ogni caso i dipendenti hanno la possibilità di concordare questa modalità con il proprio datore di lavoro, sulla base di quanto stabilito dall'accordo aziendale o un contratto collettivo nazionale. Lo stesso Ministero del lavoro ha poi precisato che il lavoro a domicilio occasionale non era soggetto ai requisiti della normativa sul posto di lavoro, ma era oggetto dell'applicazione delle disposizioni generali della legge tedesca sulla sicurezza e la salute sul lavoro. Perciò durante la fase più critica dell'emergenza sanitaria, permane l'obbligo a compiere da parte del datore di lavoro una valutazione dei rischi, di fatti rimaneva invariata l'applicazione della normativa riguardante gli infortuni sul lavoro.

Per quanto riguarda il Regno Unito, si registra un atteggiamento piuttosto prudente nei confronti di tale modalità di lavoro. Infatti, sebbene nell'ordinamento inglese è presente una normativa nazionale che consente a tutti i dipendenti, per un periodo di almeno 26 settimane, il diritto di richiedere una forma di lavoro flessibile, tra cui vi rientra anche il lavoro da remoto[50], a seguito dell'emergenza pandemica ciò che è stato compiuto è stata la redazione di un pacchetto di linee guida rivolte ai datori di lavoro. Queste linee guida rivolte a tutti i datori di lavoro suggerivano di incoraggiare tutti i dipendenti a lavorare da casa[51]. Sono state poi previste altre linee guida specifiche per una serie di settori[52]. In ogni caso il modello anglofono si caratterizza per una ancora minor presenza dell'azione governativa nella valorizzazione del lavoro da remoto, sostanzialmente l'approccio che ne emerge è quello di consentire la continuità dell'attività produttiva in sicurezza.

Anche l'approccio statunitense è piuttosto prudente nei confronti del lavoro da remoto. Il legislatore, infatti, ha sempre teso a lasciare ampia discrezionalità al datore di lavoro sulla possibilità di implementare forme di lavoro flessibile. Nell'ordinamento federale americano non è previsto un diritto al home working e non vi è nemmeno una legge che inquadri questa modalità lavorativa. Il tutto è dunque lasciato alla discrezionalità del datore di lavoro. L'unica eccezione riguarda il *Family Medical Leave Act* che riconosce ad alcuni dipendenti con condizioni mediche speciali, la possibilità di accedere al lavoro da casa. Di fronte all'emergenza Covid-19, questa disciplina non ha subito alcun tipo di modifica o implementazione, lasciando di fatti piena libertà all'azienda su come gestire l'emergenza. Da sottolineare in ogni caso come il Governo abbia predisposto una "Guida intermedia

[50] Articolo 3 del Flexible Working Regulations, entrato in vigore 30 giugno 2014
[51] Guidance for employers and business on Coronavirus (COVID-19), Department for Business Energy & Industrial Strategy, Public Health England, 7 aprile 2020.
[52] Social Distancing in the workplace during coronavirus (COVID-19): sector guidance, Department for Business Energy & Industrial Strategy, Public Health England, 7 maggio 2020

per aziende e datori di lavori per rispondere al Coronavirus"[53] al fine di sostenere le imprese nella gestione della crisi e di tutelare la salute dei lavoratori, con cui si raccomandava i datori di lavoro a stabilire politiche e pratiche per l'allontanamento sociale. La *Occupational Safety and Health Administration* ha inoltre predisposto tutta una serie di linee guida per organizzare i luoghi di lavoro in maniera funzionale ad una limitazione della diffusione del contagio.

Da questa panoramica si può cogliere la contrapposizione tra due differenti modelli. Da un lato troviamo un approccio senza dubbio più incisivo in termini di azione governativa, volto ad utilizzare il lavoro da remoto come forma di protezione per i lavoratori e di contrasto al virus, di fatto alleggerendo di molto la normativa vigente in materia e imponendola *de facto* ai datori di lavoro (modello italiano e spagnolo). Stati Uniti e Regno Unito invece, non hanno provveduto ad implementare o modificare la stessa, lasciando l'onere e l'onore al datore di lavoro di trovare la modalità di gestione più adatta al datore di lavoro. A questo modello si avvicina molto quello tedesco, mentre caso a sé è quello francese, caratterizzato da una normativa del *teletravail* già in grado di affrontare le necessità causa pandemia. Due modelli senza dubbio contrapposti ma che rispondono ad un'unica necessità: la prosecuzione delle attività produttive.

5. Il lavoro da remoto ed il potere di controllo datoriale tra privacy e valutazione del risultato

Il massiccio ricorso allo smart working ha garantito durante l'esplosione della pandemia la continuità operativa del Paese; tuttavia, il contesto in cui si deve garantire la protezione dei dati ed il potere di controllo datoriale e le mutate condizioni logistiche e strumentali della prestazione lavorativa hanno imposto attente riflessioni in varie aree in merito a soluzioni stabilmente funzionali e verso un più sostenibile equilibrio socioeconomico. In questa strenua lotta per la mitigazione della pandemia da Covid-19, numerose sono state le problematiche emerse in ambito protezione dati sottese sia alle attività di pubblico contrasto all' emergenza epidemiologica sia alla dimensione domestica in cui ciascun individuo ha sperimentato un nuovo modo di vivere la propria socialità e professionalità. Nel panorama nazionale tra le questioni ad impatto privacy di notevole interesse non possiamo non citare, in modo esemplificativo ma non esaustivo:

- Le iniziative emergenziali di sorveglianza sanitaria concordate tra parti sociali con relative problematiche concernenti le rilevazioni diagnostiche effettuabili dal datore di lavoro
- I progetti di contenimento implementati specificatamente dalle imprese verso i propri collaboratori

[53] Interim Guidance for Business and Employers Responding to Coronavirus Disease 2019 (COVID-19), Centers for Disease Control and Prevention (CDC), Maggio 2020

- Le truffe informatiche (phishing e furti di identità online ai danni di persone alla disperata ricerca di presidi di protezione o farmaci salvavita)
- Le vulnerabilità di cybersecurity evidenziate da alcune delle piattaforme di interazione sociale, professionale o scolastica
- Il grave *data breach* che ha interessato il sito dell'INPS nella partizione dedicata alle richieste di misure emergenziali di sostegno economico con mancata pronta informazione degli interessati
- L'utilizzo di droni per seguire e dissuadere i possibili trasgressori dei divieti di circolazione
- L' implementazione di sistemi di *track & tracing* della popolazione.

Un particolare rilievo in tema di lavoro da remoto, anche in questo contesto emergenziale, viene assunto dalla disciplina concernente il potere di controllo del datore di lavoro.
L'art.4 dello Statuto dei Lavoratori, come modificato dall' art.23 del D. Lgs. n.151 del 2015 ha avuto l'obiettivo di superare gli intrinseci limiti tecnologici offrendo un quadro di compatibilità con le forme di controllo, posto che l'attività in questo attuale scenario si svolge a distanza, in esterno rispetto ai siti aziendali ed in connessione remota. Risulta tuttavia evidente che gli stessi strumenti che consentono al lavoratore di erogare la prestazione diventano essi stessi funzionali all'esercizio del potere di controllo del datore di lavoro che necessariamente avrà limiti differenti rispetto a quando il lavoro viene eseguito all' interno dell'azienda.
Legittimo quindi il considerare che il cosiddetto potere di controllo nel "*remote working"* dovrà avere come focus il risultato della prestazione stessa, piuttosto che il "dove e quando" della prestazione stessa.

Nella nostra società digitalizzata il lavoratore, e certamente il lavoratore da remoto, è potenzialmente costantemente soggetto ad un controllo a distanza, potendo qualsiasi *device*, applicazione o sistema consentire indagini e analisi su varie categorie di dati, rilevando tempi, contenuti e transazioni eseguite, basti pensare alle cosiddette funzioni di *trace o log*.
Difatti i nuovi strumenti di lavoro consentono potenzialmente di tracciare e ricostruire l'intera attività svolta dal lavoratore, nonché l'accesso ad eventuali dati sensibili dello stesso, basti pensare ad esempio a quanto deducibile dall' esame dei siti internet visitati e/o dalla lettura della posta elettronica e/o dai dati di localizzazione tramite il GPS o infine tramite i *wearable device* per cui è possibile rilevare dati sensibili del lavoratore quali quelli biomedici relativi alla pressione corporea, battito cardiaco, flusso sanguigno che combinati potrebbero dare indicazioni di indice di stanchezza e stress del lavoratore stesso. Non vi è dubbio sicuramente che trattasi di dati preziosi per l'azienda ma nello stesso tempo anche una miniera di informazioni del lavoratore che se non opportunamente trattati, nel rispetto di appropriati principi di conservazione spazio-temporale rappresentano un serio pericolo per la riservatezza e la privacy del lavoratore stesso.

Il potere di controllo del datore di lavoro deve quindi necessariamente contemperare le esigenze dell'impresa con i valori di riservatezza e di dignità del lavoratore. I limiti del potere datoriale di controllo nel lavoro da remoto dovranno tenere conto dei limiti dettati dalla disciplina dell'art.4 dello Statuto dei Lavoratori come riformato dall'art.23 d.lgs.151 del 2015, e del Regolamento (UE) 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (regolamento generale della protezione dei dati).

La tutela della privacy e protezione dei dati assume rilevanza sia nell'ottica di protezione del lavoratore che in quella di tutela dell'impresa, che necessita della cooperazione del lavoratore da remoto, per la sua vulnerabilità intrinseca dovuta a potenziali attacchi informatici di terzi. Infatti, il lavoratore da remoto è tenuto ad una condotta diligente in riferimento all'utilizzo e custodia degli strumenti di lavoro e dei dati trattati, adottando misure che evitino l'accesso o la diffusione dei dati a persone non autorizzate e presenti nel luogo di esecuzione della prestazione.

Nel lavoro agile come per il potere direttivo, la regolamentazione del potere di controllo è oggetto di accordo individuale. Il legislatore affida dunque al patto individuale il compito di superare le difficoltà inerenti all'esercizio del potere di controllo in relazione ad una qualunque prestazione svolta in qualunque luogo a discrezione del lavoratore. Difatti l'art. 21.1 della legge 22 maggio 2017 n.81 prevede "che l'accordo relativo alla modalità di lavoro agile disciplina l'esercizio del potere di controllo del datore sulla prestazione resa dal lavoratore all'esterno dei locali aziendali nel rispetto di quanto disposto dall'art.4 della legge 20 maggio 1970 n.330 e successive modificazioni". Secondo la parte dottrinale maggioritaria tale art. 21.1 non limita assolutamente i poteri datoriali, quanto più attribuisce all'accordo il compito di individuare come in concreto il datore possa esercitare i propri poteri in relazione all'attività resa all'esterno dei locali aziendali, sempre attenendosi alla disciplina prevista dall'art.4 dello Statuto dei Lavoratori.

Ai nostri fini è sufficiente soffermarci sulla distinzione operata dal primo e dal secondo comma dell'art.4, ossia fra strumenti di cui si dota l'organizzazione di lavoro (comma 1) e strumenti di lavoro in dotazione al singolo dipendente (comma 2). Mentre l'installazione dei primi resta subordinata alla stipulazione di un accordo con le rappresentanze sindacali (aziendali o unitarie) o in assenza tramite apposita autorizzazione dell'Ispettorato del Lavoro, volta ad accertare l'effettiva esigenza, al contrario, gli strumenti di lavoro in dotazione al singolo lavoratore per rendere la prestazione lavorativa al pari degli strumenti di registrazione degli accessi e delle presenze ai sensi della previsione del secondo comma sono sottratti a vincoli causali e alle garanzie procedurali.

L'intenzione del legislatore è quella di liberalizzare l'uso degli strumenti di lavoro (pc, posta elettronica, telefonini, GPS, ecc.), con l'intenzione di valorizzare la consapevolezza del lavoratore che utilizza strumenti tecnologici di mettere in conto la condizione di potenziale controllo del datore. Dunque, nel lavoro da remoto è complicato rilevare strumenti di lavoro che ricadono nella disciplina del primo comma dell'art.4.

A bilanciare la disciplina dell'art. 4.2 dello Statuto dei Lavoratori è il successivo comma del medesimo articolo, che al fine di garantire la dignità e la libertà del lavoratore, stabilisce che l'utilizzabilità dei dati registrati dallo strumento tecnologico è condizionata, da un lato, dal fatto che il datore fornisca adeguata informativa in relazione alle modalità d'uso degli strumenti e dei controlli, dall'altro, che i controlli medesimi avvengano nel rispetto di quanto disposto dal d.lgs. 30 giugno 2003 n.196. L'art.4.3 impone dunque uno stretto coordinamento tra normativa giuslavoristica e privacy. L'adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli deve riguardare tanto gli strumenti previsti dal comma 1 quanto dal 2. Il terzo comma dello Statuto dei Lavoratori condiziona il trattamento dei dati al solo adempimento dell'obbligo di informativa senza richiedere alcun tipo di consenso, difatti capovolgendo la prospettiva del Codice della Privacy, in cui il consenso assume il ruolo di condizione di legittimità del trattamento. L'art 4.3 come visto, oltre a prevedere che il lavoratore debba essere informato della modalità di effettuazione dei controlli; tuttavia, non chiarisce quando tali controlli possano essere esercitati, rimandando solo al rispetto di quanto previsto d al d.lgs. 2003 n.196, modificato dal d.lgs. 2018 n.101 (adeguamento GDPR). Tale previsione impone uno stretto coordinamento tra normativa giuslavoristica e privacy, inducendo a ritenere che "il principale argine ad un utilizzo pervasivo dei controlli sul lavoro sarà nella conformità al Codice".

Il datore di lavoro sulla base del principio di *accountability* è tenuto a conservare ed organizzare i dati personali del lavoratore nel rispetto dei loro diritti alla luce della disciplina vigente e dei principi di *privacy by design* (sin dal principio qualsiasi progetto deve essere realizzato garantendo la riservatezza finale dell'utente e la protezione dei suoi dati) e *privacy by default* (i dati vengono raccolti nella minor misura possibile, di fatti espressione della minimizzazione dei dati e di limitazione della finalità). Sempre al livello generale, l'esercizio del potere datoriale di controllo deve rispettare il principio di minimizzazione del trattamento, di limitazione delle finalità e il principio di necessità (art.5 e 6 del GDPR). Inoltre, con specifico riferimento ai dati dei lavoratori, l'art.88 del GDPR attribuisce ai legislatori nazionali e alla contrattazione collettiva il compito di fissare regole più specifiche per assicurare la tutela dei diritti e delle libertà nel rispetto dei principi del trattamento dati. A tali principi generali si affiancano le disposizioni del Titolo VIII Capo III del d.lgs. n.196 del 2003 (modificato dal D. Lgs. 2018 n.101) espressamente dedicate al Controllo a distanza, lavoro agile e

telelavoro. In ogni caso solo l'osservanza di entrambe le condizioni previste dall'art.4.3 dello Statuto dei Lavoratori, dunque obbligo di informativa e rispetto della tutela della privacy, legittima il datore di lavoro all'utilizzo dei dati a tutti i fini connessi al rapporto di lavoro, in caso contrario almeno sul piano civilistico le informazioni ed i dati raccolti saranno inutilizzabili.

La progressiva liberalizzazione del potere di controllo deve essere contemperata da un orientamento restrittivo dell'Autorità garante che garantisce il principio secondo cui il datore di lavoro, pur esercitando il potere di controllo al fine di verificare l'effettivo adempimento della prestazione, deve salvaguardare la dignità e la libertà dei dipendenti. Infatti, l'Autorità garante ha precisato che l'uso di programmi che operano in background, cioè la cui esecuzione non richiede l'intervento del lavoratore e che altresì consentono la verifica in maniera costante e indiscriminata degli accessi alla rete o alla posta elettronica, sono in contrasto con la privacy e lo Statuto dei Lavoratori come confermato dalle modifiche introdotte dal Jobs Act[54]. Tra gli strumenti consentiti dal Garante, per rendere la prestazione lavorativa, vi rientrano solo servizi software o applicativi strettamente funzionali alla prestazione lavorativa (ad esempio sistemi di logging per l'esercizio del servizio di posta elettronica, sistemi di filtraggio antivirus che rilevano anomalie di sicurezza nelle postazioni di lavoro o sui server ecc.)[55]. Per quanto riguarda invece i sistemi di geolocalizzazione attivabili su supporti digitali mobili, il Garante precisa che il sistema deve essere predisposto in modo tale che sullo schermo dello smartphone sia evidente un'icona che indichi ai dipendenti quando la funzione di localizzazione è attiva. Nell'ottica di un puntuale controllo dei sistemi che raccolgano ed utilizzano dati personali del lavoratore, il Garante della Privacy con il Provvedimento n. 467 del 2018, ha incluso nell' elenco dei trattamenti da sottoporre alla valutazione di impatto sulla protezione dei dati "i trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (ad esempio sistemi di videosorveglianza e geolocalizzazione) dai quale derivi la possibilità di effettuare un controllo a distanza dell'attività del dipendente[56].

In estrema sintesi, prima di implementare soluzioni che consentano forme di controllo delle attività svolte in lavoro agile, il datore di lavoro deve:

- valutare che la tecnologia – o meglio l'utilizzo che se ne intende fare – sia conforme a quanto previsto dallo Statuto dei lavoratori

[54] Garante Privacy, Provvedimento n. 303 del 13 luglio 2016 e Garante Privacy Prov. 547/2016.
[55] Il Garante considera, quindi "strumenti di lavoro" sia il servizio di posta elettronica offerta ai dipendenti sia gli altri servizi della rete aziendale, fra cui anche il collegamento ai siti Internet, nonché i sistemi e le misure che ne consentano il fisiologico e sicuro funzionamento al fine di garantire un elevato livello di sicurezza della rete aziendale messa a disposizione del lavoratore.
[56] Con riferimento alla geolocalizzazione dei dipendenti, il Garante ha ritenuto che solo in casi estremamente rari può essere ricondotta all'eccezione di cui al secondo comma dell'art. 4 l. n. 300 del 1970, e pertanto di regola, è soggetta alla procedura codeterminativa di cui al primo comma della medesima disposizione (Cfr. Garante per la protezione dei dati personali, Relazione 2016, pag. 97 e segg., nonché i recenti provvedimenti dello stesso Garante del 16 marzo 2017, n. 138, e del 24 marzo 2017, n. 247).

- effettuare una DPIA (*Data Privacy Impact Assessment*) sui trattamenti che possono generare attività di controllo per valutarne la base giuridiche e la rispondenza ai principi di minimizzazione, proporzionalità, e al rischio residuo
- nel caso l'esito della DPIA evidenzi un rischio elevato per i diritti e le libertà dei lavoratori, e si voglia comunque procedere con l'implementazione, provare ad interpellare il Garante tramite lo strumento di consultazione preventiva di cui all' art.36 del GDPR
- informare i lavoratori sul funzionamento della tecnologia, sulle modalità di controllo e su eventuali opzioni a sua disposizione

In conclusione, dall'analisi sin qui fatta, emerge che il potere di controllo datoriale nel lavoro da remoto, anche in questo contesto emergenziale, trova come limite principale la necessità di conformarsi alla disciplina della tutela dei dati personali, che inevitabilmente incide sulla raccolta dei dati e delle informazioni. Dunque, il potere datoriale nel lavoro da remoto dovrà in ogni caso rispettare i principi di *data protection* di trasparenza, di minimizzazione, proporzionalità e progressività del trattamento, tenuto conto che la prestazione di lavoro da remoto avviene senza precisi vincoli temporali e di luogo. Infatti, la dematerializzazione del luogo di lavoro e l'orario flessibile, da un lato produce minori costi per i datori di lavoro, dall'altro realizza una miglior conciliazione della vita professionale e privata dei lavoratori, se si riesce ad imporre l'adozione di comportamenti e misura dei risultati improntati alla responsabilità e conseguimento dei risultati. Quindi le imprese dovranno adottare un nuovo modello organizzativo orientato a specifici obiettivi misurati non sul controllo della persona ma sulla qualità e sui risultati raggiunti, ad esempio, e in maniera non esaustiva, attraverso strumenti di soddisfazione dei servizi forniti verso i propri clienti interni.
La pandemia ha provocato, in modo tanto subitaneo quanto forzato, il più grande esperimento globale di smart working nella storia. Molte imprese hanno azionato un cosiddetto "*switch to remote mode*" senza avere tempo e modo di considerare adeguatamente l'introduzione di specifiche di contesto, lasciando spazio all' improvvisazione e ad una scarsa consapevolezza. Ora che siamo entrati in una fase di convivenza col virus ed in una progressiva normalizzazione, le implicazioni tra lavoro agile e normativa privacy dovranno essere oggetto di specifica valutazione e puntuale regolamentazione.

6. Tecnologie per lo smart working: osservazioni e complementi

Abbiamo visto come le tecnologie digitali rivestono un ruolo fondamentale nell'agevolare e rendere possibili nuovi modi di lavorare e sono un driver fondamentale dello stesso *Smart Working*. Esse, infatti, consentono di ampliare e rendere virtuale lo spazio di lavoro, creando un *digital workplace* in cui comunicazione, collaborazione e socializzazione sono indipendenti da orari e luoghi di lavoro. Ai fini di questa trattazione abbiamo ritenuto significativo provare a dare una risposta ai

quesiti: cosa vuol dire introdurre nuove tecnologie all'interno degli attuali modelli organizzativi? E quali sono, nella pratica, le tecnologie per lo *Smart Working*?

Una delle prime attenzioni, all'atto dell'avvio di qualsiasi iniziativa di *Smart Working*, deve essere quella di analizzare la dotazione tecnologica disponibile per comprendere la fattibilità concreta del progetto e pianificare l'eventuale introduzione dei nuovi strumenti. Troppo spesso, progetti di introduzione di tecnologie informatiche sono avviati e valutati senza tenere in considerazione i possibili impatti sul modello organizzativo, non solo in termini di processi, ma anche di implicazioni e vincoli su spazi fisici, policy organizzative e stili di leadership. In questo modo si rischia di non cogliere appieno le potenzialità dei nuovi strumenti e dell'impatto che possono avere sui comportamenti delle persone.

Anche in situazioni dove potrebbe venir meno la possibilità di avviare iniziative di *Smart Working* con un approccio sistemico, l'introduzione di tecnologie e competenze digitali è un importante prerequisito per preparare e innescare il lancio di future iniziative che vadano a modificare il modello organizzativo stesso. La vera difficoltà, infatti, non ricade nella scelta e nell'introduzione di nuovi strumenti, ma nel fare in modo che questi siano efficacemente adottati e influenzino positivamente il modo di lavorare creando nuove opportunità di relazioni e collaborazioni più mature e coinvolgenti.

Vediamo, quindi nel concreto gli ambiti tecnologici relativi allo Smart Working.

Una prima caratterizzazione delle tecnologie di *Smart Working* è che permettono alle persone di lavorare in modo flessibile sia all'esterno che all'interno delle sedi aziendali, tecnologie che possiamo raggruppare in quattro macrocategorie:

- "*Social Collaboration*"

Si tratta di strumenti che integrano e supportano i flussi di comunicazione creando nuove opportunità di relazione, collaborazione e condivisione della conoscenza come, ad esempio, strumenti di *instant messaging*, *web conference*, integrazione fisso/mobile e fruite su piattaforme diverse come PC, tablet, Smart Phone. Imparare ad utilizzare in modo corretto queste tecnologie consente di abilitare modalità di comunicazione, collaborazione e interazione con colleghi, clienti e terze parti e, quindi, tra persone che non sempre si trovano nello stesso luogo. Le iniziative di Social Collaboration permettono di limitare i trasferimenti per incontri in cui non sia fondamentale la presenza fisica fornendo un'alternativa valida alla collaborazione; questo permette di avere delle implicazioni positive per le persone e per le organizzazioni in termini, ad esempio, di costi di trasferta.

- Sicurezza e Privacy

Sono tecnologie che permettono di accedere in totale sicurezza ed in modo flessibile, semplice e immediato, un ambiente organizzativo che contiene applicativi, dati e informazioni, preservando l'integrità dei dati indipendentemente dal dispositivo adottato. In questo gruppo di servizi rientrano sia soluzioni tradizionali come l'accesso tramite *Virtual Private Network* con meccanismi di autentificazione forte (preferibilmente a due fattori) sia, soluzioni di virtualizzazione basate sul *Cloud*.

Nell'implementazione di un progetto di *Smart Working*, è fondamentale garantire la presenza di un canale sicuro per accedere anche da remoto: soluzioni volte a garantire la sicurezza dei dati inviati e ricevuti sono presenti nella quasi totalità delle grandi aziende e devono essere oggi adottate anche da quelle di piccole dimensioni. Al di là degli strumenti, tuttavia, per tutelare la sicurezza occorre anche formare le persone e renderle pienamente consapevoli dell'importanza di adottare comportamenti corretti anche e soprattutto quando lavorano in contesti di *Smart Working*, inserendo nelle sessioni formative una parte dedicata alla sicurezza e fornendo periodicamente un'informativa sui rischi connessi.

- Mobilità

È riferita a dispositivi che permettono di accedere ai servizi e agli strumenti professionali in qualunque momento e da qualunque luogo, liberando le persone dalla necessità della "postazione fissa" (es. Notebook/PC portatili, Smartphone, Tablet). Tali dispositivi vengono utilizzati sia all'esterno della sede di lavoro sia all'interno facilitando forme di mobilità strutturata.

I dispositivi mobili sono oggi presenti in tutte le grandi aziende, ma non sempre la loro diffusione tra i lavoratori è sufficiente e incide davvero sulle modalità di organizzazione del lavoro perché troppo spesso vengono assegnati più in base all'inquadramento professionale che rispetto alle specifiche esigenze organizzative.

Una soluzione che potrebbe facilitare la diffusione di tali dispositivi è l'introduzione di politiche di BYOD (*Bring-Your-Own-Device*) che prevedono la possibilità da parte dei lavoratori, nell'ambito di specifici accordi, di utilizzare i propri device personali per accedere ad alcune applicazioni aziendali. Questo approccio ha il vantaggio di permettere alle persone di utilizzare strumenti mobili che ben sanno utilizzare per svolgere alcune attività a tutto vantaggio dell'efficacia e della flessibilità di luogo. Dal punto di vista della sicurezza le politiche di BYOD in ogni caso molto spesso sono

disincentivate dalle aziende a favore di soluzioni già predisposte dall'azienda e non liberamente modificabili dall'utente come, ad esempio, soluzioni di Virtual Desktop o PC/Smart Phone gestiti dall'azienda.

- Workspace Technology

Si fa riferimento a tutte quelle tecnologie che permettono un utilizzo più efficace e flessibile degli ambienti fisici agevolando non solo la fruibilità degli spazi stessi, ma anche supportando il lavoro in mobilità delle persone e migliorando la qualità della vita all'interno delle sedi dell'azienda come ad esempio i sistemi Wi-Fi, i sistemi e gli strumenti che consentono di fare videoconferenze, sistemi di Telepresence, Print Area centralizzate, che consentono di operare su qualsiasi stampante inserendo le proprie credenziali o utilizzando il proprio badge aziendale per confermare la stampa.

Nelle grandi organizzazioni, a prescindere dalla presenza o meno di un progetto di *Smart Working*, le tecnologie che supportano il lavoro da remoto sono già diffuse: in modo particolare le soluzioni a supporto della sicurezza e dell'accessibilità dei dati da remoto e da diversi dispositivi e le iniziative di *mobilità*, come ad esempio la presenza di *device* mobili e *mobile business app*. Molto spesso inoltre sono presenti servizi di *social collaboration* integrati a supporto della collaborazione e della condivisione della conoscenza, mentre meno diffuse sono le *workspace technology* che permettono un utilizzo più flessibile degli ambienti agevolando il lavoro in mobilità all'interno delle sedi aziendali.

A fronte della presenza nelle aziende di questi strumenti, tuttavia, la loro reale diffusione e capacità di utilizzo tra i lavoratori è spesso inadeguata a consentire a tutti di lavorare da remoto o in mobilità interna con sufficiente efficacia e sicurezza. La dotazione tecnologica standard per consentire il lavorare da remoto si compone principalmente di PC portatile, VPN e servizi di *social collaboration*. Solo quando necessari vengono introdotti device mobili come smartphone e tablet. In ogni caso non è sufficiente l'introduzione di nuove tecnologie affinché sia supportato efficacemente il cambiamento culturale che lo *Smart Working* richieda; talvolta emergono alcune criticità.

Le principali barriere che limitano oggi la capacità delle tecnologie digitali nel supportare le iniziative di *Smart Working* riguardano:

- la non ancora completa digitalizzazione dei processi aziendali;
- la scarsa efficacia nella comunicazione e collaborazione virtuale;

- le difficoltà dovute alla capacità di assicurare lo stesso livello di performance dei sistemi anche al di fuori della sede aziendale.

Anche quando la dotazione tecnologica di partenza non è ottimale, tuttavia, l'avvio di iniziative di *Smart Working* consentono di metter in luce la necessità di nuovi strumenti e applicazioni che hanno poi un effetto positivo che va al di là del loro utilizzo nell'ambito dello *Smart Working* stesso.

Dal punto di vista del "Diritto del lavoro" come recentemente osservato dal Prof. De Masi[57], si passerà dal "diritto del lavoro" al "diritto per il lavoro" dato che il cittadino, grazie alla strutturazione del lavoro per progetti, passa da "salariato di massa" a produttore di beni e servizi: a ciò consegue che il concetto di lavoro subordinato si avvicinerà sempre più a quello di lavoro autonomo. In realtà la potenziale rivoluzione conseguente al lavoro da remoto guarda in realtà al passato, essendo fondata sul "sogno antico" di un "lavoro a misura d'uomo", il quale è stato distrutto nel momento in cui l'avvento del capitalismo industriale ha causato l'espulsione degli artigiani dalle proprie "case-bottega" e li ha costretti a lavorare nelle fabbriche.

Per quanto concerne il passaggio strategico da lavoro rigido ad agile nel settore pubblico dipende principalmente dalla qualità della dirigenza, dall'implementazione di idonei sistemi di sicurezza informatica e soprattutto da una forte volontà in tal senso da parte della politica. Perché, tale trasformazione possa avverarsi, serve altresì un incremento di competenze digitali dei dipendenti, realizzabili grazie a investimenti mirati sulla formazione e al ricambio generazionale.

[57] DE MASI D. *Smart Working. La rivoluzione del lavoro intelligente* 2020 Marsilio Editore

CAPITOLO IV
EMERGENZA PANDEMICA E PROCESSO DI ADEGUAMENTO DELLE IMPRESE

1. Gestone della Crisi: "Crisis Management"

In questo delicato frangente pandemico molte aziende hanno sperimentato e stanno ancora sperimentando la gestione di una crisi pandemica senza precedenti. Nella vita di ogni impresa è probabile, spesso fisiologico, trovarsi a fronteggiare una situazione di emergenza più o meno inaspettata, la chiave del successo, in questi casi, è essere pronti a gestirla, con un piano mirato di gestione delle crisi: il piano di *Crisis Management*.

Con *Crisis Management* si intende il processo attraverso cui un'impresa affronta una situazione che rischia di procurare danno (materiale e di immagine) mettendo in atto una serie di pratiche che consentono di prevenire, gestire e mitigare gli effetti della crisi. Il *Crisis Management Board* è la funzione strutturale del processo di direzione di un'organizzazione, medio o grande, che analizza, predispone e coordina la gestione di situazioni di crisi.

Il *Crisis Management* è un processo di medio/lungo periodo, che incorpora tutte le varie attività da svolgere prima, durante e dopo un evento negativo in modo tale da tutelare l'azienda da minacce e ridurne l'impatto critico. In questo modo si va a intervenire su inevitabili falle nell'interruzione del normale funzionamento delle attività, fronteggiando l'avanzare della crisi.

Un piano di *Crisis Management* è basato su un approccio e una cultura mirati alla preparazione alla gestione della crisi. L'attenzione alla prevenzione e l'individuazione dei potenziali scenari di crisi è l'arma più intelligente di cui un'azienda può dotarsi per prevenire e limitare i danni.

Risultano elementi chiave da tenere in considerazione:

- La rilevazione degli indicatori di problematiche che possono/potrebbero comportare l'insorgere di rischi per l'organizzazione;
- La valutazione del grado di effettiva preparazione della squadra nel gestire l'emergenza;
- L'attribuzione nella squadra di ruoli e compiti da svolgere in caso di crisi, formando il personale e preparandolo ad ogni possibile scenario.

Il processo di gestione della crisi si suddivide in tre fasi principali:

- ***RESEARCH***:
  si va a ricercare limiti, mancanze e vulnerabilità che mettono a rischio il business, elaborando un piano di gestione della crisi.
- ***RESPONSE***:
  si studiano *feedback* e capacità di adattamento dell'azienda al piano messo in atto, valutando rimedi a possibili ulteriori incidenti on-the-job.
- ***RECOVERY***:
  nella fase di ripresa, si mette in atto quelle azioni volte a ripristinare lo *status quo*, minimizzando (dove possibile) i danni occorsi.

Ovviamente, ogni crisi è a sé stante, ed è impossibile redigere un piano di azioni univoco: sfumature e obiettivi saranno sempre differenti. Pertanto, monitorare costantemente l'andamento dell'azienda, individuando possibili falle nel sistema e soluzioni si dimostra la tecnica vincente per non farsi trovare impreparati all'arrivo di una crisi. Durante la fase di gestione di un evento critico, gli strumenti di cui un'azienda può avvalersi sono molteplici. Alcuni però sono di fondamentale importanza e dovranno essere costituiti e migliorati continuamente.
La *business continuity* di un'azienda dovrebbe venire pianificata seguendo il cosiddetto *Deming Cycle*, detto anche "ciclo PDCA". Questo strumento parte dall'assunto che per il raggiungimento della massima qualità è necessaria una costante interazione di quattro fasi:

- P – Plan (programmazione): viene elaborata una lista di possibili aree di crisi e un'ipotesi di procedura per risolverle;
- D – Do (esecuzione): la procedura viene applicata secondo il programma, effettuando simulazioni di scenari di crisi;
- C – Check (test e controllo): lo studio e la raccolta dei risultati di feedback derivanti dall'applicazione e la procedura;
- A – Act (azione): il processo viene migliorato sulla base del feedback ottenuto e quindi reso definito e ampliato in tutto il suo ambito di applicazione.

Il modello viene fatto applicare direttamente dal personale aziendale, individuando le diverse predisposizioni personali e seguendo le modalità di selezione del *crisis team*. Il primo passo da compiere per prepararsi all'eventualità di una crisi è quello di individuare il *crisis team*, anche detto comitato di crisi, cellula di crisi o, con riferimento al luogo fisico dove si svolgono le riunioni in occasione della crisi, *crisis room*.

Questa squadra organizzata di lavoro ha la funzione di svolgere direttamente le varie fasi di *Deming Cycle*, effettuando quindi un lavoro di prevenzione e gestione degli eventi negativi che potranno colpire l'organizzazione. La selezione della squadra dipende molto dal tipo di attività svolta dall'azienda, dalla sua struttura organizzativa e dai vari livelli di cui essa è composta. Le competenze di base richieste sono eterogenee, alcune sono direttamente interpellate in riferimento a situazioni specifiche o in base a loro conoscenze particolari del settore, ad esempio il manager diretto dell'area in cui si verifica la crisi.

È fondamentale quindi che ogni *team* sia adeguato alla particolare situazione di crisi, ovvero che all'interno dell'azienda ci siano diversi team adatti alle diverse tipologie di crisi.

Alcuni dei membri imprescindibili all'interno del crisis management team sono:

- CEO (Amministratore delegato);
- vicepresidente;
- responsabile finanza e controllo
- responsabile del personale;
- responsabili degli affari legali;
- funzione sicurezza e privacy;
- funzione salute e sicurezza;
- qualità;
- logistica;
- ufficio stampa;
- responsabile di relazioni pubbliche.

Queste figure, nella maggior parte dei casi, vengono selezionate all'interno dell'organizzazione, in casi specifici invece, come per esempio nei casi di eventi critici coinvolti in più mercati è necessario riferirsi a una *task force* esterna specializzata che, in questo caso, conosca particolarmente bene la cultura e le leggi dello Stato di riferimento.

Le funzioni principali del *crisis team* sono ripartite nei tre momenti temporali della crisi in prima, durante e dopo l'evento critico. Quelle iniziali si esauriscono nell'analisi delle aree vulnerabili, nel monitoraggio dei segnali deboli e nella stesura del piano di crisi. Le attività durante la crisi sono quelle di gestione e di comunicazione dell'evento, volte in particolare ad assicurare la qualità strategica del processo decisionale attraverso l'analisi di una vasta gamma di variabili, come la precisazione dei costi, dei rischi, obiettivi e valori in gioco. Quelle successive all'evento, infine,

riguardano le azioni di recupero e di rilancio, oltre alla stesura di un documento che ripercorra tutte le tappe della gestione della crisi appena avvenuta e la riscrittura del piano di crisi aggiornato

Nel presidio della Crisi Pandemica il *Crisis Board* per aziende medie e grandi è stato la chiave fondamentale per tenere sotto controllo i rischi, i costi e gli impatti derivanti dalle continue variazioni normative dettate dallo stato di emergenza e garantire continuità di business nel rispetto e tutela della salute dei lavoratori e della loro privacy.

2. Protocollo condiviso

Nell'attuale situazione legata all' emergenza epidemiologica, i datori di lavoro, al fine di contenere il contagio, nell'ottica dell'attuazione delle misure anti-contagio sul luogo di lavoro previste dalla normativa emergenziale in atto, sono chiamati ad osservare le misure per il contenimento e la gestione dell'emergenza contenute nel "Protocollo condiviso di regolamentazione delle misure per il contrasto ed il contenimento della diffusione SARS-CoV-2/COVID-19 negli ambienti di lavoro" tra Governo e parti sociali che aggiorna e rinnova i precedenti accordi , su invito del Ministro del lavoro e delle politiche sociali e del Ministro della salute, tenuto conto dei precedenti provvedimenti adottati. Il documento è stato realizzato per agevolare gli enti e le imprese nell' adozione di protocolli di sicurezza anti-contagio, negli ambienti di lavoro, contenendo importanti disposizioni anche in materia privacy. Di queste misure e degli obblighi previsti dalla normativa emergenziale le imprese devono dare adeguata informazione ai propri dipendenti e agli eventuali visitatori esterni (clienti, fornitori, etc.), anche tramite apposite informative, cartellonistiche all'ingresso dei locali e specifici protocolli interni e/o vademecum comportamentali.

Le principali raccomandazioni contenute nel protocollo sono in relazione a:

- Informazione
- Accesso alla sede di lavoro
- Igiene in azienda
- Spazi comuni e spostamenti
- Organizzazione aziendale
- Gestione di una persona sintomatica in azienda
- Sorveglianza sanitaria, Medico competente e RLS.

In particolare, si indica, con riferimento al DPCM 2 marzo 2021, che le misure restrittive per le attività di produzione raccomandano:

- "*il massimo utilizzo, ove possibile, della modalità di lavoro agile o da remoto da parte dei datori di lavoro privati, ai sensi dell'articolo 90 (Lavoro agile) del decreto-legge 19 maggio 2020, n. 34, convertito, con modificazioni, dalla legge 17 luglio 2020, n. 77, nonché di quanto previsto dai protocolli 12 e 13 allegati al citato DPCM 2 marzo 2021;*
- *che le attività professionali siano attuate anche mediante modalità di lavoro agile, ove possano essere svolte al proprio domicilio o in modalità a distanza;*
- *che siano incentivate le ferie e i congedi retribuiti per i dipendenti nonché gli altri strumenti previsti dalla contrattazione collettiva;*
- *che siano sospese le attività dei reparti aziendali non indispensabili alla produzione;*
- *che siano assunti protocolli di sicurezza anti-contagio, fermo restando l'obbligo di utilizzare dispositivi di protezione delle vie respiratorie previsti da normativa, protocolli e linee guida vigenti;*
- *che siano incentivate le operazioni di sanificazione nei luoghi di lavoro, anche utilizzando a tal fine forme di ammortizzatori sociali;*
- *che sull'intero territorio nazionale tutte le attività produttive industriali e commerciali rispettino i contenuti del Protocollo condiviso di regolamentazione delle misure per il contrasto e il contenimento della diffusione del virus COVID-19 negli ambienti di lavoro, nonché, per i rispettivi ambiti di competenza, il Protocollo condiviso di regolamentazione per il contenimento della diffusione del COVID-19 nei cantieri, sottoscritto il 24 aprile 2020 fra il Ministro delle infrastrutture e dei trasporti, il Ministro del lavoro e delle politiche sociali e le Parti sociali, e il protocollo condiviso di regolamentazione per il contenimento della diffusione del COVID-19 nel settore del trasporto e della logistica sottoscritto il 20 marzo 2020*".

Rimandando ad una lettura del protocollo nella sua interezza si riportano, in maniera indicativa e non esaustiva, i seguenti punti relativi al protocollo nazionale per gli ambienti di lavoro:

- Necessità di adozione di protocolli anti-contagio aziendali, "di dettaglio" rispetto a quelli nazionali, anche in riferimento alle linee guida e a quanto disposto dalla normativa vigente per gli specifici settori di attività. Informazione dei lavoratori sulle regole da adottare e sul corretto uso dei DPI forniti;
- Raccomandazione del ricorso al "lavoro agile / lavoro da casa", ove possibile;

- Fermo restando l'obbligo di mantenimento del distanziamento interpersonale, obbligo di indossare appositi dispositivi di protezione delle vie aeree negli ambienti comuni e comunque qualora non sia possibile mantenere il distanziamento interpersonale;
- Necessità di esposizione / consegna di depliant informativi ai lavoratori / terzi / fornitori circa le regole anti-contagio da seguire;
- Possibilità di controllo della temperatura corporea di lavoratori e di terzi, nel rispetto della privacy;
- Divieto di accesso agli ambienti in caso di sintomi febbrili, simil-influenzali o in caso di contatto stretto con soggetti positivi a COVID-19 nei precedenti 14 giorni;
- I lavoratori positivi oltre il ventunesimo giorno potranno essere riammessi al lavoro solo dopo negativizzazione dimostrata da tampone molecolare o antigenico effettuato in struttura accreditata o autorizzata dal Servizio Sanitario;
- Necessità di pulizia giornaliera e sanificazione periodica degli ambienti di lavoro, di pulizia a fine turno e sanificazione periodica di tastiere, schermi touchscreen e mouse;
- Effettuazione di opportuni interventi di sanificazione straordinaria degli ambienti ove hanno soggiornato casi COVID-19;
- Non sono consentite riunioni in presenza, se non motivate da oggettive impossibilità di effettuazione con modalità "a distanza" o da carattere di urgenza e necessità;
- Rimangono consentite solo alcune tipologie di corsi di formazione "in presenza", fra i quali quelli aziendali e quelli in materia di salute e sicurezza, questi ultimi anche multi-aziendali;
- Necessità di sottoporre i lavoratori positivi a COVID-19 che hanno subito un ricovero ospedaliero, indipendentemente dalla durata dello stesso a visita medica precedente alla ripresa dell'attività lavorativa.

Ripercorrendo il testo, si evidenzia che restano invariate l'impostazione e la struttura della precedente versione del Protocollo e senza alcun dubbio non ci sono variazioni rilevanti per gli ambiti data protection e privacy se non in termini di processo con le implicazioni derivanti dalla conferma del ruolo del medico competente nel trattamento dei dati particolari e nella tutela dei lavoratori fragili.

Nel rispetto della previsione dell' art. 29 bis della legge n.40/2020, che individua nelle previsioni del Protocollo il contenuto concreto dell' art. 2087 del codice civile, come indicato nella Nota di Aggiornamento di Confindustria: "la finalità era quella di acquisire nel documento le novità normative e scientifiche (previsioni di legge, circolari esplicative, evoluzione delle conoscenze in relazione, soprattutto, alle varianti) per attualizzare le regole di sicurezza contro l' epidemia e

semplificarne l' applicazione per le imprese, superando previsioni non più attuali ed in contrasto con leggi e circolari sopravvenute della nuova versione di questo Protocollo".

Le misure di sicurezza stringenti conseguono e sono in relazione alle varianti, la cui virulenza amplia il rischio di contagio, potenziando l'uso potenziato della mascherina, si riduce il rischio di contagio ed attivazione del contact tracing e quindi si riduce le ipotesi di diffusione del virus al di fuori dei luoghi di lavoro, in famiglia e nella società limitando quindi isolamento e quarantena. Si richiama il ruolo del medico competente nella tutela dei lavoratori fragili, con richiamo espresso della circolare del 4 settembre 2020 e nella proposta di adozione, di strategie di testing/screening, tenendo conto della circolare n. 705 dell'8 gennaio 2021.Per contatto stretto, si fa riferimento alla circolare del Ministero della salute del 29 maggio 2020, e si richiama l'esigenza che, al fine di rendere efficace il tracciamento secondo le peculiarità aziendali, la relativa identificazione avvenga tenendo conto delle misure di prevenzione e protezione individuate ed attuate in azienda, rispettando sotto il profilo privacy quanto già previsto.

In tema di riammissione al lavoro, il Protocollo aggiornato prevede espressamente che la visita al rientro è prevista "per il reintegro progressivo dei lavoratori già risultati positivi al tampone con ricovero ospedaliero". La disposizione prevede dunque la visita al rientro solamente in caso di pregressa ospedalizzazione, ed appare, quindi, limitata rispetto alla portata generale che ispirava l'originaria previsione del Protocollo. Questa precisazione sembra sollevare l'azienda da un onere di accertamento nelle ipotesi "minori", quali asintomatici, assenza di gravità, assenza di ricovero ospedaliero, tuttavia introduce questioni afferenti alla privacy: il datore di lavoro può non sapere se la persona è stata ospedalizzata e non supera, non escludendola espressamente, la possibilità di effettuare sempre e comunque la visita al rientro. Autorevoli interpretazioni ritengono che continui ad essere rimessa alla valutazione del medico competente l' opportunità di effettuare le visite al rientro nelle ipotesi diverse da quelle indicate nella circolare n. 14915 del 29 settembre 2020 dal Protocollo.

In conclusione, il Protocollo nella sua nuova versione presenta elementi di adeguamento alle novità giuridiche ed alle conoscenze scientifiche, conservando autonomia rispetto alla materia di sicurezza del lavoro senza introdurre elementi di variazione rispetto agli ambiti di adeguamento privacy. Quanto all' efficacia dello stesso, esso è stato recepito con l'ordinanza del 21/5/2021 del Ministero della Salute.

3. Misure contenitive ed Impatti Privacy: Misurazione della temperatura corporea, Autodichiarazioni, Test sierologici

L' emergenza pandemica ha indotto modifiche e cambiamenti con riferimento alla privacy nel rapporto di lavoro. Nell'ottica dell'attuazione delle misure anti-contagio sul luogo di lavoro previste dalla normativa emergenziale in atto dal "Protocollo condiviso di regolamentazione delle misure per il contrasto ed il contenimento della diffusione SARS-CoV-2/COVID-19 negli ambienti di lavoro" e, prima, in particolare, dal "Protocollo condiviso di regolamentazione delle misure per il contrasto e il contenimento della diffusione del virus Covid-19 negli ambienti di lavoro" del 14 marzo 2020, poi integrato e sostituito dal Protocollo del 24/04/2020, le imprese sono tenute ad adottare una serie di misure necessarie a tutelare la salute delle persone presenti all'interno dell'azienda e a garantire la salubrità degli ambienti di lavoro. Di queste misure e degli obblighi previsti dalla normativa emergenziale le imprese devono dare adeguata informazione ai propri dipendenti e agli eventuali visitatori esterni (clienti, fornitori, etc.), anche tramite apposite informative, cartellonistiche all'ingresso dei locali e specifici protocolli interni e/o vademecum comportamentali.

Come abbiamo visto in precedenza, dopo il rigido approccio iniziale di inizio marzo il Garante Privacy, sulla scorta della linea adottata dal Comitato Europeo per la protezione dei dati (EDPB), ha precisato che la normativa privacy non ostacola l'adozione delle misure per il contrasto della pandemia di Coronavirus. Tuttavia, anche in questi momenti eccezionali le imprese devono garantire la protezione dei dati dei lavoratori eventualmente raccolti e/o comunque trattati, tramite opportuni accorgimenti. Infatti, l'attuazione di determinate misure di contenimento del rischio di diffusione del virus Covid-19 all'interno delle aziende può comportare la raccolta o comunque il trattamento di dati "particolari" dei lavoratori o delle persone fisiche (ad esempio quelli relativi allo stato di salute), come avviene nel caso di rilevazione della temperatura corporea, di raccolta di autodichiarazioni in merito al soggiorno o meno in zone a rischio epidemiologico o su contatti o meno con persone risultate positive al COVID-19.

Il trattamento di tali dati, alla luce dell'attuale contesto emergenziale e del conseguente nuovo quadro normativo, è quindi da considerarsi legittimo ma, nondimeno, comporta la necessità, da parte dell'azienda, di adottare i dovuti accorgimenti al fine di porre in essere un trattamento di dati nel rispetto della vigente normativa in materia di privacy. Pertanto, in qualità di Titolare del trattamento, l'impresa dovrà quindi definire le misure di sicurezza tecniche e organizzative adeguate a proteggere tali dati, provvedendo anche ad individuare e formalmente incaricare i soggetti autorizzati al trattamento e fornendo loro le istruzioni necessarie.

Nello specifico, al fine di ottemperare al citato Protocollo in atto le imprese che si avvarranno della facoltà di rilevare la temperatura corporea all'ingresso dei propri locali (N.B.: nei cantieri però è un obbligo) oppure che concederanno ai propri dipendenti l'opportunità di sottoporsi a test sierologici su base volontaria in conformità ad eventuali delibere di Giunta (a titolo esemplificativo ad es. per la regione Emilia Romagna possiamo citare la delibera n. 350 del 16/04/2020 per le imprese ubicate in Emilia Romagna), dovranno in particolare adeguare la propria documentazione privacy richiesta dal Regolamento Europeo n. 2016/279 (GDPR). Ciò significa, in concreto:

1. fornire una idonea informativa privacy con l'indicazione degli elementi fondamentali del trattamento e, in particolare, le nuove finalità legate alla gestione dell'emergenza Coronavirus, le basi giuridiche su cui si fonda il trattamento, i tempi di conservazione dei dati, ecc.;
2. redigere apposite lettere di incarico, con relative istruzioni, da fornire al personale interno autorizzato al trattamento dei dati (ci sono infatti precisi limiti nella gestione dei dati, pertanto occorre precisare ciò che è consentito e ciò che non lo è);
3. valutare la designazione scritta quali responsabili del trattamento dei dati dei soggetti "esterni" (sulla base di un atto giuridico di nomina) eventualmente incaricati di effettuare questa attività sulla base di un contratto di servizio.

Si tratta quindi in ossequio al principio fondamentale di accountability (responsabilizzazione) introdotto dal GDPR, di attivare un processo di Privacy Impact Analysis, che consenta, in estrema ratio di implementare e documentare le misure e le azioni poste in essere, preventivamente all' attuazione del trattamento dei dati in conformità alla normativa vigente.

Oltre alla modulistica di cui ai punti 1), 2) e 3) sopra elencati, occorre prevedere la predisposizione, anche della seguente documentazione:

- Registri da utilizzare per l'accesso in azienda previa rilevazione della temperatura (uno per dipendenti e uno per utenti esterni), nel rispetto di appropriate misure di sicurezza;
- Autodichiarazione circa la non provenienza da zone a rischio epidemiologico o l'assenza di contatti, negli ultimi 14 giorni, con soggetti risultati positivi al COVID-19, con informativa privacy;
- Vademecum comportamentale sulle misure anti-contagio da Covid-19, per dipendenti;
- Cartellonistica riassuntiva da affiggere all'ingresso dei locali.

Si sottolinea in particolare che riguardo alla modalità di ingresso in azienda, come già previsto nel Protocollo condiviso del 24 aprile 2020, che gli aspetti connessi alla protezione dei dati personali sono stati trattati nelle note a piè di pagina, con riferimento al paragrafo relativo alle modalità di

ingresso in azienda, fornendo indicazioni relativamente all'eventuale trattamento di dati personali, qualora il datore di lavoro subordini l'accesso ai locali aziendali alla misurazione della temperatura corporea e/o all'acquisizione di ulteriori dati attraverso il rilascio di dichiarazioni attestanti la non provenienza da zone a rischio epidemiologico e l'assenza di contatti negli ultimi 14 giorni con soggetti risultati positivi al Covid-19.

Allo scopo di dare risposta ad una serie di quesiti manifestati sulle problematiche connesse all'emergenza derivante dal Covid-19, con particolare riferimento al trattamento dei dati nel contesto lavorativo pubblico e privato, il Garante per la protezione dei dati personali si è, espresso fornendo ulteriori chiarimenti e indicazioni operative, nell'ambito delle proprie "FAQ", che tengono conto delle risposte fornite nonché dei reclami, segnalazioni e quesiti raccolti.

Una delle misure messe in atto dalle imprese ai fini di prevenzione del contagio da COVID-19 ad impatto privacy risulta la introduzione della misurazione della temperatura corporea, all'ingresso dei locali aziendali, dei dipendenti nonché di soggetti terzi, quali fornitori, clienti e visitatori. In primis si rileva che, ad eccezione di alcuni ambiti territoriali o specifici settori, in relazione ai quali la misurazione della temperatura corporea è stata individuata come obbligatoria, come, ad esempio, nel caso della Regione Lombardia, con le ordinanze n. 546 e n. 547 emanate nel mese di maggio 2020 e nel caso del Protocollo condiviso per la regolamentazione per il contenimento della diffusione del Covid-19 nei cantieri" , l'adozione di tale misura è stata prevista su base facoltativa, anche se, successivamente alle prime fasi della pandemia, si sono intensificate le raccomandazioni per la relativa implementazione, in ragione del rischio di riattivazione di focolai nei luoghi di lavoro.

Dal punto di vista della Data Protection, comportando tale misura il trattamento di dati personali e, per di più, di dati relativi alla salute, appartenenti alle categorie particolari di dati, si è posta attenzione ai relativi impatti sulla tutela dei dati personali e sulle modalità di attuazione della stessa. A questo riguardo, già nel "Protocollo condiviso di regolamentazione delle misure per il contrasto e il contenimento della diffusione del virus Covid-19 negli ambienti di lavoro fra Governo e parti sociali", la cui prima versione risale al 14 marzo 2020, per limitare in capo al datore di lavoro/titolare del trattamento le relative conseguenze ed oneri, è previsto che di regola non sia effettuata alcuna registrazione dei dati inerenti alla temperatura corporea, ad eccezione dei soli casi di superamento della temperatura-soglia, ove la registrazione del dato sia necessaria per documentare le ragioni ostative all'accesso al luogo di lavoro. In proposito, le sopraindicate "FAQ" del Garante hanno ulteriormente ribadito questo aspetto, con un espresso richiamo all'osservanza del principio di minimizzazione.

In linea con quanto sopra, il Garante ha, altresì, specificato come la registrazione del dato, nel caso di misurazione della temperatura corporea a soggetti terzi (ad es. clienti o visitatori), non sia necessaria, anche laddove la temperatura risulti superiore alla soglia.

Le imprese nell' implementazione della misura in questione, nel rispetto dei protocolli, delle indicazioni del Garante, dei principi e delle prescrizioni della normativa per la protezione dei dati personali, hanno dovuto porre in essere una serie di adempimenti tra cui la predisposizione di informative per l'accesso ai locali aziendali e la misurazione della temperatura corporea - accompagnate da avvisi informativi/raccomandazioni esposti all'ingresso dei locali aziendali – e l'introduzione di specifiche misure organizzative, finalizzate ad istruire e autorizzare (ai sensi dell'art. 29 del GDPR e per le imprese italiane dell'art. 2-quaterdecies del "Codice in materia di protezione dei dati personali"), il personale al trattamento dei dati in questione.

Tale misura, ampliamente applicata da parte delle imprese, è stata oggetto di appositi interventi da parte di Autorità di controllo al fine di garantire il bilanciamento tra diritto alla salute, tutela della riservatezza e diritto alla protezione dei dati personali. Il titolare con riferimento al proprio contesto potrebbe considerare di effettuare una valutazione di impatto, in ossequio all' art.35 del GDPR, in caso di trattamenti su larga scala di categorie particolari di dati personali.

Altra misura che pone richieste di attenzione in ambito privacy è l'autocertificazione, da far sottoscrivere ai propri dipendenti, e, in taluni casi, anche a soggetti terzi, quali clienti, fornitori e visitatori. Una tale prassi necessita attente considerazioni, sia per la raccolta di documenti cartacei sia per il trattamento di dati personali, in particolare quelli relativi alla salute nel rispetto del principio di minimizzazione.

Non banale, risulta poi l'introduzione da parte dei datori di lavoro di tecnologie più complesse, sempre per la rilevazione della temperatura, quali le termo camere. In tal caso sia alla luce delle disposizioni di protezione dati che in tema di controllo dei lavoratori risulta fondamentale una valutazione preliminare in merito alle caratteristiche tecniche di tali strumenti.

In ambito data protection il titolare deve considerare dall' integrazione del registro dei trattamenti, allo svolgimento di una valutazione di impatto, alla designazione dei soggetti autorizzati ad accedere ai dati in caso di superamento della soglia della temperatura, alle istruzioni e formazione degli stessi, alla nomina dei soggetti responsabili dei trattamenti, alla redazione di una specifica informativa.

Un'ulteriore misura adottata dalle imprese e tra l'altro non specificamente prevista nei Protocolli riguarda la messa a disposizione del personale test sierologici. Attente valutazioni di impatto anche in questo caso risultano fondamentali. Il Garante ha precisato che, nell'ambito del sistema di

prevenzione e sicurezza sui luoghi di lavoro o di protocolli di sicurezza anti-contagio, tale misura possa essere adottata "solo se disposta dal medico competente", chiamato, in particolare, a "suggerire l'adozione di mezzi diagnostici, qualora ritenuti utili al fine del contenimento della diffusione del virus e della salute dei lavoratori". Inoltre, sempre in ottica data protection, il Garante ha rilevato come i dati relativi alla diagnosi o all'anamnesi familiare dei lavoratori non debbano essere oggetto di trattamento da parte dei datori di lavoro (fatta eccezione per i dati relativi al giudizio di idoneità alla mansione specifica e alle eventuali prescrizioni o limitazioni stabilite dal medico competente) e che, oltre alle campagne di screening avviate dalle autorità sanitarie competenti, il datore possa, sostenendone in tutto o in parte, i relativi costi, proporre ai propri dipendenti l'effettuazione di test sierologici, senza in ogni caso poter conoscere l'esito dei test.

Risulta evidente che le misure poste in essere ai fini di prevenzione del contagio da COVID-19 comportano una serie di oneri e responsabilità, destinati ad assorbire le imprese in svariati ambiti, non solo quello economico. Gli adempimenti che gravano sul datore di lavoro sono notevoli sia come misure implementative finalizzate al contenimento contagi sia per l'accesso alle sedi sia per l'erogazione del servizio da remoto, quando applicabile, come già trattato nell' apposito capitolo.

4. Checklist di monitoraggio adempimenti nell' applicazione di due case studies

Quale inevitabile conseguenza di quanto esposto nei precedenti paragrafi, le imprese hanno reagito prontamente, attuando al proprio interno le prescrizioni contenute nei protocolli e, in taluni casi, anche andando oltre il perimetro dagli stessi individuato, adottando strumenti e misure non espressamente previsti.

L'attuazione delle suddette misure non è stata, tuttavia, priva di criticità, non solo di carattere operativo ma anche tecnico/giuridico, tra cui vanno compresi i conseguenti impatti sul fronte data protection. La disciplina vigente vieta la diffusione dei dati relativi alla salute. Tale divieto non è stato derogato dalla normativa d'urgenza epidemiologica da COVID-19 per finalità di contenimento della diffusione dell'epidemia.

Solo a fini rilevatori nell'ambito organizzativo e produttivo della società sono stati presi a campione due realtà: un' azienda dell' area logistica *FIUMICINO LOGISTICA EUROPA S.R.L.U., soggetta a direzione e coordinamento di BCUBE Air Cargo S.p.A. FLE, ubicata all'interno dell'aerostazione merci (Cargo City) dell'Aeroporto internazionale "Leonardo Da Vinci "Fiumicino (RM)* ed un ente ecclesiastico che opera a livello internazionale nella promozione della cultura della fraternità universale, tratteggiando e raccogliendo con l'ausilio di un questionario la loro risposta in

tema di adeguamento e revisione di processi, elaborazione di nuove procedure ed azioni implementative sottese dagli adempimenti previsti per fronteggiare la crisi pandemica.

Nel corso di questo lavoro, gli approfondimenti che ne sono derivati sono risultati un osservatorio privilegiato, completamente proteso ad evidenziare eventuali elementi che, nella gestione della crisi pandemica e relativi impatti sulla protezione dei dati dei lavoratori, sarebbero potuti emergere da queste esperienze tratte direttamente dal vivo del tessuto produttivo aziendale e dall'irrinunciabile necessità di garantire un servizio alle persone anche durante la crisi pandemica.

In termini di considerazioni conclusive, indipendentemente dal protrarsi o meno della crisi pandemica, emerge che alcuni elementi di novità introdotti nei processi, nell' organizzazione e nelle attività stesse, fortemente accelerati da questa prolungata emergenza, quale il *remote working* e l'impiego delle video conferenze per le assemblee deliberative e le riunioni di lavoro, sicuramente potranno continuare ad essere utilizzati per alcune tipologie di attività e per determinate figure professionali già abituate a lavorare per obiettivi con una propria autonomia decisionale ed in grado di fornire riscontri strutturati e ricorrenti. In questo periodo la tecnologia ha fatto da driver per l'innovazione del modello organizzativo. Difatti senza alcuni strumenti tecnologici disponibili, specificatamente hardware, software, sicurezza, connettività e applicazioni utili al lavoro in team, sarebbe stato impossibile garantire la continuità nella produzione e nella prestazione dei servizi in modo efficace garantendo altresì la protezione dei dati dei lavoratori.

Checklist a cura di FIUMICINO LOGISTICA EUROPA S.R.L.U.

id	Domande	Risposte a cura dell'azienda
0.	breve descrizione della società e del mercato di riferimento (va bene anche sito istituzionale) ed ok ad usare i dati qui riportati in tabella e/o aggregati e sintetizzati nella tesi	*FIUMICINO LOGISTICA EUROPA S.R.L.U.* *FLE è ubicata all'interno dell'aerostazione merci (Cargo City) dell'Aeroporto internazionale "Leonardo Da Vinci" Fiumicino (RM).* *Attività prevalente: Assistenza merci e posta per le merci esportate, importate o in transito. Movimentazione fisica delle merci.* *http://www.fle-roma.it*
1.	In riferimento alla pandemia di SARS-COV2 la vostra azienda ha attivato un comitato di gestione della crisi? Covid Crisis Management Team	*Si*
2.	Se SI:	
2.1	Composizione del comitato in termini di funzioni aziendali coinvolte (CEO, DG, HR, Finance, IT, OHS, etc ....)	*Il Comitato Interno Covid è stato costituito ad alto livello strategico con: Datore di Lavoro , RSPP di sito (HSE), RSPP di gruppo (HSE Manager), HR Manager, Dirigenti Delegati alla Sicurezza.* *Il Comitato Interno Covid è stato poi esteso a: HR di sito, Medico Competente di sito, RLS di sito e RSA di sito.*
2.2	Chi guida il comitato? Security - DG - etc . (Driver e Sponsor)	*Il Comitato è guidato dal Datore di Lavoro, RSPP e HR Manager*
2.3	Frequenza dei meeting del comitato (settimanle, quindicinale, mensile, a seconda dei momenti di crisi ....)	*A seconda dei momementi di crisi.*
2.4	Vengono prodotte minute dei meeting e le informazioni più importanti comunicate ai dipendenti?	*Vengono emessi Verbali Interni di Comitato Covid-19 condivisi con Medico Competente, RLS e le RSA di sito.*
2.5	E' stato prodotta un area informativa di consultazione interna dove vengono riportate news, linee guida, gestione viaggi, etc (es. Tramite specifica porzione di Intranet aziendale)?	*Attraverso la diffusione via e-mail vengono condivisi gli aggiornamenti dei protocolli interni (Istruzioni di Salute e Sicurezza, HSE/HR Notice, ecc..) e gli aggiornamenti normativi. Le informative e le procedure sono disponibili sulle bacheche aziendali e sulle cartelle intranet.*
2.6	Quali iniziative principali sono state adottate dal comitato per il contenimento dell'epidemia? (misurazione temperatura, controllo accessi, smart working, contigentamento accessi, etc...)	*Tutte le misure individuate nei protocolli interni sono state preventivamente discusse e condivise in sede di comitato per il contenimento dell'epidemia.*
2.7	Come è stato gestito il trattamento dei dati sensibili dei dipendenti, external workforce e dei fornitori/clienti?	*Nessun dato personale particolare è stato rregistrato e conservato. Le modalità di trattamento dei dati (relativi a temperatura corporea, non provenienza da zone a rischio epidemiologico e assenza di contatti stretti) sono state diffuse a tutti mediante informativa ai sensi dell'art. 13 Reg (UE) 2016/679 (GDPR).Il trattamento dei dati è stato affidato esclusivamente a medico competente e personale hr specificatamente individuato dall'azienda. I dati non sono trattenuti se non per il tempo strettamente necessario in caso di richiesta da parte dell'autorità sanitaria per la ricostruzione della filiera degli eventuali contatti e comunque non oltre la fine dello stato di emergenza.*
3.	Se NO	
3.1	Come è stata gestita la crisi ? Una particolare funzione aziendale ha avuto la responsabilità della gestione? Chi?	
3.2	E' stato prodotta un area informativa di consultazione interna dove vengono riportate news, linee guida, gestione viaggi, etc (es. Tramite specifica porzione di Intranet aziendale)	
3.3	Quali iniziative principali sono state adottate dal comitato per il contenimento dell'epidemia? (fornitura di Dispositivi di Protezione Individuali -DPI; misurazione temperatura, controllo accessi, smart working, contigentamento accessi - max 10 % -30% di posti di lavori, etc...)	
3.4	Come è stato gestito il trattamento dei dati sensibili dei dipendenti, external workforce e dei fornitori/clienti?	
4.	E' stato implementato un protocollo condiviso per la gestione della pandemia in accordo al protocollo del ministero della salute al link sotto riportato?	
4.1	Covid-19 - Lavoratori e imprese	
5.	Potete descrivere la procedura/processo di rilevazione della temperatura ai dipendenti e terze parti?	*La rilevazione della temperatura a dipendenti e terze parti viene effettuata mediante termoscanner ubicato in ingresso Carg-City, il controllo è affidato al personale incaricato dal Gestore Aeroportuale. Il processo è descritto con apposita procedura interna IASS- RILEVAZIONE TEMPERATURA INGRESSO LUOGHI DI LAVORO.*
6.	Potete descrivere brevemente il piano di emergenza adottato?	*FLE ha stabilito apposita procedura di emergenza in caso di manifestazione sintomi a lavoro che attiva il piano di emergenza interno per il primo soccorso. La procedura IASS- MANIFESTAZIONE SINTOMI IN AZIENDA prevede l'uscita immediata della persona sintomatica con limitazione dei contatti e ove necessario supporto dei sanitari esterni.*
7.	Potete descrivere il processo di gestione viaggi durante la pandemia?	*Il processo è descritto mediante apposita procedura IASS- GESTIONE TRASFERTE E VIAGGI. I viaggi sono autorizzati previa verifica di DL, HR e RSPP delle misure preventive e protettive da adottare in funzione dello stato emergenziale.*
8.	Potete descrivere le politiche di accesso ai vostri uffici per dipednenti e terze parti?	*è vietato l'accesso di esterni negli uffici ove non strettamente necessario. È vietato l'accesso di corrieri negli uffici. Le modalità di accesso sono definite in apposito Protocollo Covid..*
9.	Smart Working - SW (Lavoro Agile)	
9.1	L'azienda adottava già lo SW o aveva attivato un pilota per lo SW?	*No*
9.2	All'inizio della pandemia l'azienda ha adottato meccanismi di lavoro agile?	*L'azienda ha adottato lo SW a partire dal 9 marzo 2020. Questo sarà attivo per tutte le funzioni amministrative e dirigenziali per tutta la durata dello stato di emergenza.*
9.3	I processi aziendali erano già pronti per l'adozione dello SW su scala sensibile?	*No*
9.4	I sistemi Informativi erano adeguati allo SW su larga scala o si è dovuti intervenire con soluzioni/architetture ad hoc?	*Si è dovuti intervenire con soluzioni ad hoc*
9.5	Avete chiesto ai dipendenti con un questionario interno se lo SW ha avuto benefici o meno ?	*Si*
9.6	L'azienda ha tratto benefici dallo SW?	*Si*
9.7	Pensate di adottare in maniera corposa lo SW anche dopo la pandemia?	*Si*
10	Potete descrivere dal punto di vista privacy le iniziative prese e tese a proteggere il lavoratore durante la pandemia?	*Nessuna raccolta dei dati sensibili. Comunicazione dei dati sensibili solo attraverso il medico competente o ufficio HR.*
11.	Potete descrivere come sono stati gestiti i dati sanitari nel contesto lavorativo e di privacy?	*Vedi sopra risposta 2.7*
12.	Oltre l'emergenza: pros and cons e elementi positivi su cui fare leva (es: SW, business continuity plan, etc)	*Training a distanza con uso di piattaforme per videoconferenze.*

Checklist a cura dell'Ente Ecclesiastico P.A.F.O.M: Movimento dei Focolari

id	Domande	Risposte a cura dell'azienda
0.	breve descrizione della società e del mercato di riferimento (va bene anche sito istituzionale) ed ok ad usare i dati qui riportati in tabella e/o aggregati e sintetizzati nella tesi	L'ente ecclesiastico Pia Associazione Femminile "Opera di Maria" è espressione civile in Italia del Movimento dei Focolari che ha come fine specificico la fratellanza universale sulla base del più pieno rispetto verso le diverse convinzioni religiose, i grandi valori umani-cristiani di giustizia sociale, libertà, solidarietà, pace. Sito web di riferimento: https://www.focolare.org/
1.	In riferimento alla pandemia di SARS-COV2 la vostra azienda ha attivato un comitato di gestione della crisi? Covid Crisis Management Team	E' stato adottato un Comitato di gestione della crisi per attuare il Protocollo di regolamentazione delle misure per il contrasto e il contenimento della diffusione del virus Covid-19 del 13 maggio 2020.
2.	Se SI:	
2.1	Composizione del comitato in termini di funzioni aziendali coinvolte (CEO, DG, HR, Finance, IT, OHS, etc ....)	Le persone coinvolte sono due procuratori speciali e due rappresentanti dei lavoratori per la sicurezza
2.2	Chi guida il comitato? Security - DG - etc . (Driver e Sponsor)	Il Comitato delibera collegialmente
2.3	Frequenza dei meeting del comitato (settimanle, quindicinale, mensile, a seconda dei momenti di crisi ....)	Il Comitato si riunisce a seconda delle necessità organizzative e nei momenti di crisi
2.4	Vengono prodotte minute dei meeting e le informazioni più importanti comunicate ai dipendenti?	Le decisioni vengono comunicate ai Dirigenti che a loro volta le comunicano ai dipendenti tramite e-mail.
2.5	E' stato prodotta un area informativa di consultazione interna dove vengono riportate news, linee guida, gestione viaggi, etc (es. Tramite specifica porzione di Intranet aziendale)?	Esiste uno spazio sul portale collaboration@focolare.org. Ogni ufficio e settore si è organizzato creando proprie bacheche interne per le comunicazioni
2.6	Quali iniziative principali sono state adottate dal comitato per il contenimento dell'epidemia? (misurazione temperatura, controllo accessi, smart working, contigentamento accessi, etc...)	E' stato redatto un Protocollo che prevede una serie di norme comportamentali: uso obbligatorio della mascherina chirurgica, misurazione della temperatura, controllo degli accessi, divieti di ingresso per soggetti risultati positivi o provenienti da zone a rischio, smart working, contigentamento accessi, igienizzare gli strumenti comuni utilizzati, sanificazione e pulizia, escluso l'accesso ai visitatori, i reparti non necessari restano chiusi, sospensione delle riunioni, obbligo a casa se con febbre oltre 37,5 e gestione di un caso sintomatico.
2.7	Come è stato gestito il trattamento dei dati sensibili dei dipendenti, external workforce e dei fornitori/clienti?	E' stata fornita una informativa privacy sul trattamento dei dati personali
3.	Se NO	
3.1	Come è stata gestita la crisi ? Una particolare funzione aziendale ha avuto la responsabilità della gestione? Chi?	Il Comitato ha gestito la crisi individuando per ogni settore una persona di riferimento preparata ad applicare il Protocollo adottato
3.2	E' stato prodotta un area informativa di consultazione interna dove vengono riportate news, linee guida, gestione viaggi, etc (es. Tramite specifica porzione di Intranet aziendale)	Si come indicato al punto 2.5
3.3	Quali iniziative principali sono state adottate dal comitato per il contenimento dell'epidemia? (fornitura di Dispositivi di Protezione Individuali -DPI; misurazione temperatura, controllo accessi, smart working, contigentamento accessi - max 10 % -30% di posti di lavori, etc...)	Eventi formativi ai dipendenti, la fornitura di dispositivi di Protezione Individuali, auto-misurazione temperatura, controllo accessi, smart working, contigentamento accessi, una persona al massimo per stanza e nel caso di più lavoratori si sono predisposte barriere di plaxigas e obbligo di mascherina
3.4	Come è stato gestito il trattamento dei dati sensibili dei dipendenti, external workforce e dei fornitori/clienti?	Si come indicato al punto 2.7
4.	E' stato implementato un protocollo condiviso per la gestione della pandemia in accordo al protocollo del ministero della salute al link sotto riportato?	Si è stato adottato un apposito Protocollo con schede a seconda delle aree di attività.
4.1	Covid-19 - Lavoratori e imprese	
5.	Potete descrivere la procedura/processo di rilevazione della temperatura ai dipendenti e terze parti?	Termoscanner
6.	Potete descrivere brevemente il piano di emergenza adottato?	Nel caso in cui una persona presente sviluppi febbre e sintomi di infezione respiratoria quali la tosse, lo deve dichiarare immediatamente al proprio responsabile dell'ufficio e si dovrà procedere - in base alle disposizioni dell'autorità sanitaria - al suo isolamento e a quello degli altri presenti nei locali. Il Centro procede immediatamente ad avvertire le autorità sanitarie competenti (vedi "Indicazioni e norme di comportamento per l'epidemia da coronavirus di data 10 marzo 2020" a cura del Movimento dei Focolari). La persona al momento dell'isolamento deve essere subito dotata, ove già non lo fosse, di mascherina chirurgica. L'addetto alla sorveglianza deve farsi guidare dalle istruzioni del 112. A cura del responsabile dell'ufficio spetta l'informazione delle eventuali persone che sono venute in contatto con la persona sintomatica.
8.	Potete descrivere le politiche di accesso ai vostri uffici per dipendenti e terze parti?	L'ingresso prevede la registrazione del dipendente, che è munito di mascherina,
9.	Smart Working - SW (Lavoro Agile)	E' stata una novità introdotta a causa dell' emergenza sanitaria. Tutti i lavoratori hanno lavorato da remoto e sono stati forniti degli strumenti necessari per lavorare da casa. Negli uffici a turno era assicurata la presenza di una o due persone.
9.1	L'azienda adottava già lo SW o aveva attivato un pilota per lo SW?	NO
9.2	All'inizio della pandemia l'azienda ha adottato meccanismi di lavoro agile?	SI immediatamente ha adottato lo SW
9.3	I processi aziendali erano già pronti per l'adozione dello SW su scala sensibile?	SI, si era precedentemente preparata la possibilità di lavorare in SW attraverso il Cloud aziendale.
9.4	I sistemi Informativi erano adeguati allo SW su larga scala o si è dovuti intervenire con soluzioni/architetture ad hoc?	Si sono perfezionati dei processi in corso, avendo precedentemente fatto una apposita formazione ai dipendenti sulla Disciplina della sicurezza informatica, ed in data 19 marzo 2020 tutti i dipendenti hanno ricevuto l'apposito disciplinare.
9.5	Avete chiesto ai dipendenti con un questionario interno se lo SW ha avuto benefici o meno ?	No, non è stato fatto un questionario ad hoc ma sono in corso riflessioni e valutazioni sull'argomento.
9.6	L'azienda ha tratto benefici dallo SW?	In corso di valutazione
9.7	Pensate di adottare in maniera corposa lo SW anche dopo la pandemia?	In corso di valutazione
10	Potete descrivere dal punto di vista privacy le iniziative prese e tese a proteggere il lavoratore durante la pandemia?	come risposto al punto 2.7
11.	Potete descrivere come sono stati gestiti i dati sanitari nel contesto lavorativo e di privacy?	E' stato gestito ogni caso dal medico competente del lavoro con la responsabile del personale
12.	Oltre l'emergenza: pros and cons e elementi positivi su cui fare leva (es: SW, business continuity plan, etc)	Per ora si sta continuando nel tempo di emergenza, e con pieno utilizzo dello sw, che però risulta adatto per alcuni tipi di lavoro, ma non in generale. Si sta valutando la possibilità di permettere ai dipendenti che lo richiedono uno o due giorni di sw. Un punto chiave per l'ente è il lavoro in squadra, e la presenza fisica dei dipendenti, anche se non a tempo pieno, si sente importante. La (per ora) lenta ripresa della convegnistica richiederà speriamo a breve per i dipendenti interessati la presenza sul luogo di lavoro.

Si include per comodità il file excel completo:

Tesi Labriola - info aziende.xlsx

5. Lavoro Agile: Un'esperienza di gestione emergenza pandemica attraverso la remotizzazione del lavoro

Nel corso di questo studio tra le esperienze aziendali considerate per gli approfondimenti in riferimento alla gestione dell'emergenza pandemica attraverso la remotizzazione del lavoro riportiamo per dimensioni ed importanza l'esperienza Enel SpA[58].

Enel è un'azienda elettrica multinazionale, leader integrata nei mercati globali dell'energia, gas e fonti rinnovabili, trattasi della più grande utility europea in termini di EBITDA (margine operativo lordo) ordinario ed è presente in oltre 30 paesi nel mondo, producendo energia con oltre 88 GW di capacità gestita. Enel ha introdotto lo smart working per rispondere ad esigenze di miglioramento del bilanciamento vita lavoro dei dipendenti, riduzione del tempo, dei costi e delle emissioni legate agli spostamenti tra casa ed ufficio e miglioramento ed ottimizzazione delle modalità di lavoro, quali attività di condivisione delle informazioni e collaborazione.

L'esperienza dello smart working in Enel è iniziata a giugno 2016, con un pilota in Italia che ha coinvolto circa 500 dipendenti. Il progetto è stato progressivamente esteso, nel 2019 su circa 70.000 dipendenti in tutto il mondo, oltre 17.000 lavoravano in remoto per un giorno a settimana. L' azienda in fase di avvio ha provveduto ad identificare le attività aziendali compatibili col lavoro smart e definire la popolazione elegibile. In Italia lo smart working è stato regolato da un accordo sindacale il 4 aprile 2017, in cui si è individuata come finalità dello smart working l'incremento della produttività e l'agevolazione della conciliazione vita lavoro, prevedendo la volontarietà di adesione nell' ambito delle unità individuate dall' azienda, con la possibilità di lavorare da remoto massimo un giorno a settimana da concordare col proprio responsabile. La giornata di lavoro agile è equiparata a tutti gli effetti di legge e di contratto ad una giornata di "orario normale" di lavoro.
Delega, responsabilità e sicurezza nell' organizzazione del lavoro sono stati alla base del processo di change management. Il progetto di smart working è stato affiancato da iniziative di digitalizzazione dei processi:

- Per la parte infrastrutturale, il 100% degli impianti di generazione sono monitorati da remoto
- La relazione col cliente è stata oggetto di progressiva digitalizzazione

[58] MARTONE M. (a cura di), *Il Lavoro da Remoto – Per una riforma dello smart working oltre l'emergenza* 2020, Tribuna d'Autore pp. 249-255.

Per le infrastrutture IT, il Gruppo ha trasferito tutti i sistemi e le infrastrutture aziendali in architettura cloud. In tale contesto non sono stati necessari nuovi investimenti per abilitare lo smart working, in quanto il 75% dei dipendenti era già dotato di pc portatile e telefono aziendale.
In funzione dell'emergenza Covid-19, e grazie alle precedenti iniziative già definite e testate, Enel ha abilitato in pochi giorni, oltre 37 mila dipendenti nel mondo allo smart working, tutti i giorni della settimana e garantendo la continuità operativa.
Per monitorare e gestire tutte le attività e le problematiche legate all' emergenza. il Comitato di Crisi è stato attivato per il presidio delle stesse. Dapprima si è deliberata la pianificazione di una turnazione nelle sedi più popolose, ripartendo il personale in 50% da remoto e 50% in sede, per poi chiudere dal 12 marzo tutte le sedi, convertendo in remoto il 99% delle attività degli impiegati, consentendo di lavorare in smart working il 55% della popolazione aziendale. Per gli operativi (es. operai) per cui la remotizzazione non risultava applicabile, si è definito un programma di "cellularizzazione", il personale è stato diviso in squadre isolate tra di loro, senza condivisione di spazi comuni e con percorsi di accesso ed uscita separati.

In Italia, il 27 marzo 2020 è stato firmato l'Accordo sindacale per la regolamentazione degli operai dell'azienda impegnati in attività non remotizzabili in ottica di sicurezza legata all' emergenza Covid-19, con riduzione e sospensione attività, prevedendo per i periodi di inattività, giornate di permesso retribuito con recupero. Enel ha istituito una banca dei giorni lavorativi, con una donazione dei giorni lavorativi pari al numero dei dipendenti al fine di ridurre le giornate di permesso per i periodi di inattività dovuti dall' emergenza, gli stessi lavoratori potevano contribuire donando una o più giornate di ferie. L' azienda ha inoltre ai fini di bilanciamento tra vita privata e professionale alimentato una serie di iniziative ed opportunità professionali e culturali.

Il 9 giugno 2020 è stato siglato il nuovo accordo sindacale riguardante le linee guida sullo smart working e le misure per contrastare rischi di isolamento ed un sano equilibrio tra lavoro e tempo libero. Le modalità, secondo cui i lavoratori durante la fase emergenziale possono esser chiamati a fornire la propria prestazione sono:

- smart working prolungato, per chi svolge attività remotizzabili e può prevedere l'accesso alle sedi aziendali o presso terzi con carattere occasionale e comunque concordato con il responsabile;
- smart working alternato prolungato, per chi svolge attività che possono essere effettuate alternativamente da casa e da sedi aziendali o di terzi (es. clienti, fornitori). Le alternanze possono essere bi-settimanali, settimanali o infrasettimanali

Tra le misure organizzative al fine di promuovere il benessere e l'utilizzo della modalità di lavoro agile e la disconnessione dalle strumentazioni tecnologiche di lavoro, fuori dai normali orari di lavoro, sono state individuate le seguenti:

- pianificazione delle attività nell' arco del normale orario di lavoro di riferimento
- rispetto della pausa pranzo evitando riunioni in quell' arco temporale
- invio e-mail durante la fascia temporale lavorativa, evitando la fascia serale/notturna, il weekend e i giorni festivi
- alternanza tra momenti di sedentarietà e momenti dedicati a piccole ad attività motorie

Gli obblighi di informativa sulla sicurezza ai sensi della previsione di legge sono stati assolti per via telematica. Secondo quanto dichiarato dall'azienda, a partire da questa esperienza si stanno studiando nuovi modelli operativi e modalità di lavoro che diventeranno parte del "new normal".

"L' obiettivo è quello di superare la modalità di lavoro tradizionale, che vede gli uffici come il luogo per lavorare, muovendosi verso modalità di lavoro sempre più smart, dove gli uffici diventano una delle opzioni piuttosto che la soluzione di default valida per tutti i giorni, in una chiave di complementarità tra funzioni gestite a distanza e funzioni gestite in presenza".

6. Green Pass nel contesto lavorativo

Il Green pass per l'accesso ai luoghi di lavoro, oltre ad essere un tema di stringente attualità in questo contesto storico caratterizzato dalla pandemia, è un tema sempre più rilevante nel dibattito complessivo della privacy. Come espresso dal Presidente dell'Autorità per la protezione dei dati personali, la centralità di questo diritto nel contesto pandemico è tale che, sin dalle primissime misure adottate dal Governo (e dai Governi, non solo europei) a fini di contenimento dei contagi, si è dovuto anzitutto comprendere come poter coniugare esigenze di sanità pubblica e riservatezza individuale. Proprio la pandemia ha però potuto dimostrare, mettendola alla prova giorno per giorno, la funzione sociale della protezione dati, valorizzata dal GDPR sin dai suoi primi "Considerando".
Sull' uso del "Green Pass"[59] nel contesto lavorativo, iniziano ad emergere i primi profili di contrasto tra i provvedimenti del Garante Privacy e le pronunce di alcuni Tribunali nazionali in riferimento ai due temi strettamente correlati: vaccinazione obbligatoria ed esibizione del Green pass.

[59] D.L. 22 aprile 2021, n. 52 Art. 9

Mentre l'Autorità Garante Privacy, ritiene che l'esibizione obbligatoria del Green pass per l'accesso ai luoghi di lavoro da parte del dipendente debba necessariamente essere prevista da una norma di rango primario, attualmente inesistente, alcuni giudici ritengono che, in realtà, questa norma sia già presente nel nostro ordinamento giuridico e, oltre all'esibizione del Green pass, sia sufficiente a fondare l'imposizione dell'obbligo di vaccinazione al dipendente. Ragion per cui risulta di notevole complessità la valutazione dell'impatto giuslavoristico, e di conseguenza anche organizzativo, della eventuale determinazione di uno o più dipendenti di non aderire alla campagna di vaccinazione anti Covid-19 o, comunque, di non esibire il green pass eventualmente richiesto dal datore di lavoro per accedere fisicamente al luogo di lavoro. Come sappiamo, alla data, sul piano generale, nel nostro ordinamento sembra prevalere la tutela della libertà individuale del lavoratore (e dei cittadini in generale) di scegliere se sottoporsi o meno, al vaccino.

Solo con riferimento a particolari categorie di lavoratori, identificate sulla base delle mansioni svolte, e dei relativi settori di riferimento, il legislatore bilanciando i molteplici interessi coinvolti da queste attività, considerando il rischio di contagio per terzi a contatto con i lavoratori, è intervenuto introducendo uno specifico obbligo di vaccinazione. Infatti l'art.4 del D.L n. 44 del 2021 ha introdotto l'obbligo di vaccinazione anti Covid-19 esclusivamente per "*gli esercenti le professioni sanitarie e gli operatori di interesse sanitario che svolgono la loro attività nelle strutture sanitarie, sociosanitarie e socio-assistenziali, pubbliche e private, nelle farmacie, parafarmacie e negli studi professionali".* Alla data, è stato introdotto l'obbligo di esibizione del green pass per ciò che attiene il personale scolastico (insegnanti, personale ATA e dirigenti scolastici), con D.L. 6 agosto 2021, n. 111 "Misure urgenti per l'esercizio in sicurezza delle attività scolastiche, universitarie, sociali e in materia di trasporti".

Negli ambienti di lavoro, per categorie differenti da quelle su citate. dunque, alla data, non è stato introdotto dal nostro legislatore uno specifico obbligo di vaccinazione.

Numerose, tuttavia, sono state le misure predisposte per promuovere e sostenere l' adesione dei lavoratori alla campagna vaccinale, dall' azione promozionale di campagna di vaccinazione nei luoghi di lavoro promossa attraverso l' adozione del "Protocollo nazionale per la realizzazione dei piani aziendali finalizzati all' attivazione di punti straordinari di vaccinazione anti SARS-COV2/COVID-19 sui luoghi di lavoro", inoltre le aziende stesse hanno adottato specifiche misure volte ad agevolare le adesioni dei propri dipendenti che contemplano riconoscimenti di permessi retribuiti a copertura dell' assenza dal servizio collegata alla vaccinazione e suoi effetti.

Posto quindi il contesto generale per cui:

- il Governo, con il D.L. n. 105 del 2021, oltre a differire il termine del periodo emergenziale al 31 dicembre 2021, promuove l'utilizzo del c.d. "green pass", certificato comprovante: lo stato di avvenuta vaccinazione contro il COVID-19 (in tal caso il green pass ha una validità di nove mesi a far data dal completamento del ciclo vaccinale); l'avvenuta guarigione da COVID-19, con contestuale cessazione dell'isolamento prescritto in seguito ad infezione da SARS-CoV-2 (in tal caso il green pass ha una validità di sei mesi a far data dall'avvenuta guarigione); l'effettuazione di test antigenico rapido o molecolare con esito negativo al virus SARS-CoV-2 (in tale ultimo caso il green pass ha una validità di quarantotto ore dall'esecuzione del test);
- l'esibizione del c.d. "green pass", ferma restando la libertà di non vaccinarsi, è condizione, a far data dal 6 agosto 2021, per l'accesso ad alcuni servizi e attività, tra cui: a) servizi di ristorazione svolti da qualsiasi esercizio, per il consumo al tavolo, al chiuso; b) spettacoli aperti al pubblico, eventi e competizioni sportive; c) musei, altri istituti e luoghi della cultura e mostre; d) piscine, centri natatori, palestre, sport di squadra, centri benessere, anche all'interno di strutture ricettive, limitatamente alle attività al chiuso; e) sagre e fiere, convegni e congressi; f) centri termali, parchi tematici e di divertimento; g) centri culturali, centri sociali e ricreativi, limitatamente alle attività al chiuso e con esclusione dei centri educativi per l'infanzia, compresi i centri estivi, e le relative attività di ristorazione; h) attività di sale gioco, sale scommesse, sale bingo e casinò; i) concorsi pubblici;
- sebbene il Governo non abbia introdotto alcun obbligo di vaccinazione di portata generale la mancata immunizzazione, o per altro verso la certificazione di un test negativo, preclude al cittadino un numero crescente di attività che, almeno in parte, sono replicate anche negli ambienti di lavoro (si pensi, solo per fare un esempio, a punti di ristoro e mense aziendali, ai convegni e congressi);
- Confindustria ha assunto una specifica posizione diramando, in data 16 luglio 2021, una nota interna con la quale, al fine di tutelare tutti i lavoratori e lo svolgimento dei processi produttivi nel pieno rispetto delle libertà individuali, ha proposto l'estensione dell'utilizzo dei c.d. "green pass" per accedere ai contesti aziendali/lavoristici. L'approccio, in buona sostanza, ipotizza che le condizioni personali certificate tramite green pass possano assurgere a requisito necessario per legittimare lo svolgimento della prestazione lavorativa;
- si apprende da dichiarazioni pubbliche del Governo che sono in corso confronti tra le Parti sociali per definire le modalità di utilizzo del green pass anche negli ambienti di lavoro.

premessa quindi l'inesistenza di un obbligo di vaccinazione riferito agli ambienti di lavoro ed in attesa che il dialogo tra le Parti sociali indichi una linea di comportamento esigibile, è indubbio che

il Garante per la protezione dei dati personali ha assunto una posizione contraria rispetto alla possibilità per il datore di lavoro possa, anche tramite la richiesta del Green pass acquisire il dato sanitario relativo alla vaccinazione di un dipendente o comunque il suo stato sanitario di guarito con contestuale cessazione dell'isolamento prescritto o ancora di soggetto risultato negativo al tampone rapido o molecolare.

Il Garante[60] attraverso le FAQ pubblicate in data 17 febbraio 2021, ha delineato la sua posizione per cui il datore di lavoro, nonostante gli oneri di cui è gravato, non può acquisire neanche con il consenso del dipendente o tramite il medico competente tale dato sanitario, potendo acquisire in base al quadro normativo vigente i soli giudizi di idoneità alla mansione specificati dal medico competente. Tale posizione è stata ulteriormente confermata dal provvedimento emesso in data 22 luglio 2021[61], per cui l'Autorità ha avvertito la Regione Sicilia circa le criticità privacy dell'ordinanza regionale con la quale veniva previsto l'invito formale a vaccinarsi da parte della Regione a tutti i dipendenti a contatto col pubblico, a seguito di ricognizione circa l'avvenuta vaccinazione. In tale provvedimento, il Garante sottolinea che l'unica base giuridica che può introdurre un obbligo vaccinale generalizzato è una norma di legge che rispetti i principi del GDPR e sia conforme alla ripartizione dei ruoli privacy come disciplinati dal Testo Unico sulla Sicurezza nei luoghi di lavoro, di fatto secondo l'Autorità:
"certificazioni attestanti l'avvenuta vaccinazione (e, non diversamente la guarigione da Covid-19, o l'esito negativo di un test antigenico o molecolare) non possono essere ritenute una condizione necessaria per consentire l'accesso a luoghi o servizi o per l'instaurazione o l'individuazione delle modalità di svolgimento di rapporti giuridici se non nei limiti in cui ciò è previsto da una norma di rango primario."

Tratteggiata la linea dell'Autorità Garante per la protezione dei dati personali, d' altro canto considerata la specificità del rapporto di lavoro e della sua peculiare disciplina per cui:

a) in capo al datore di lavoro, ai sensi dell'art. 2087 cod. civ., ricade l'obbligo, stringente di porre in essere tutte le misure idonee a garantire la sicurezza e l'integrità psico-fisica del lavoratore all' interno dei luoghi di lavoro. La mancata vaccinazione può incidere sulle condizioni di salute e sicurezza del soggetto non vaccinato e di altri dipendenti, in particolare quelli qualificati come fragili. Una violazione di tale obbligo espone il datore di lavoro ad una responsabilità civile e /o penale

[60] Coronavirus e protezione dei dati - FAQ - Garante Privacy
Green Pass (certificazioni verdi) - Garante Privacy
[61] Provvedimento del 22 luglio 2021 - Avvertimento Regione Siciliana [9683814] - Garante Privacy

b) in riferimento all' art. 8 della legge 300 del 1970 il datore di lavoro, può acquisire legittimamente dal lavoratore tutte le informazioni dotate di rilevanza ai fini del contratto di lavoro in quanto rilevanti "ai fini della valutazione dell'attitudine professionale del lavoratore". Potrebbe rientrare quindi anche il dato relativo alla vaccinazione. Secondo la Cassazione "sono ammissibili tutte le indagini anche su fatti privati e qualità personali, utili ad accertare la competenza, la preparazione e la compatibilità col *facere* affidato" (Cass. n.2683 del 1990). Ad analoga conclusione si può pervenire considerando il dato relativo alla vaccinazione ai sensi dell'art. 9 del GDPR "un dato relativo alla salute". In tal caso si ha legittimo trattamento qualora il trattamento sia necessario "per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale e nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri".

appaiono quindi in antitesi con la posizione del Garante per la protezione dei dati personali le prime pronunce di alcuni Tribunali sul tema.

Sebbene esse non riguardino specificamente l'esibizione del Green pass, tali pronunce trattano il tema correlato della vaccinazione obbligatoria imposta dal datore di lavoro come condizione per esercitare la prestazione lavorativa.

In materia, i Tribunali di Modena, Belluno, Verona e Pavia hanno tutti recentemente bocciato i ricorsi di lavoratori no-vax. Vero è che quest'ultimi erano lavoratori di RSA, dunque sanitari, però alcune delle pronunce facevano riferimento a fatti occorsi prima dell'entrata in vigore del decreto-legge che imponeva ad essi la vaccinazione. Delle tre, la più significativa risulta quella del Tribunale di Modena, che con ordinanza del 19 maggio 2021 e successiva conferma con decreto del 23 luglio 2021[62] , ha ritenuto legittima la sospensione dalla prestazione di lavoro di due dipendenti di una RSA in seguito al rifiuto di sottoporsi al vaccino contro il Covid-19, in cui si legge che "Il datore di lavoro si pone come garante della salute e della sicurezza dei dipendenti e dei terzi che per diverse ragioni si trovano all'interno dei locali aziendali e ha quindi l'obbligo ai sensi dell'art. 2087 del codice civile di adottare tutte quelle misure di prevenzione e protezione che sono necessarie a tutelare l'integrità fisica dei lavoratori."

[62] Bollettino Adapt n. 29/2021 sez. *Labour Lawyers*: Tribunale di Modena, decreto di rigetto 23 luglio 2021, n. 2467
La mancata vaccinazione, pur non assumendo rilievo disciplinare, comporta conseguenze in ordine alla valutazione oggettiva dell'idoneità alle mansioni. È legittima la sospensione dal lavoro e della retribuzione

Il contrasto con la posizione assunta dal Garante in materia di Green pass risulta evidente. Per il Tribunale, l'articolo 2087 del codice civile è più che sufficiente a fondare la possibilità del datore di prevedere l'obbligo di vaccinazione (e quindi i correlati trattamenti di dati sanitari, per quanto da parte del medico competente) mentre per l'Autorità, tale non è.

Dai principi sino ad ora affermati dalla giurisprudenza di merito, e tenuto conto delle mansioni svolte dai lavoratori e dal contesto organizzativo di riferimento, si possono quindi ipotizzare alcune misure nella gestione del personale che rifiuti di esibire il green pass eventualmente richiesto dal datore di lavoro:

- adibizione a mansioni equivalenti o inferiori nel rispetto del 2103 c.c. che non prevedono contatto con pubblico, colleghi e terzi;
- svolgimento della prestazione in modalità agile purché il contenuto delle mansioni sia compatibile e continuino ad avere, per il datore di lavoro, un valore economicamente apprezzabile;
- richiesta del green pass per i servizi aziendali per i quali è normativamente richiesto il green pass.

Iniziative più drastiche in caso di necessità potranno essere considerate come ad esempio la collocazione del dipendente in ferie forzate (rif. Tribunale di Verona, sentenza del 24 maggio 2021, n.4469[63] e rif. Tribunale Pavia, ordinanza 20 luglio 2021[64]). Tuttavia ulteriori misure più estreme quali la sospensione della retribuzione, destinate ad incidere significativamente sulla prestazione e sui connessi diritti dei lavoratori, allo stato attuale, presentano profili di consistente incertezza in assenza di una specifica norma, o un accordo tra le Parti sociali, che ad esempio sancisca l' obbligo di vaccinazione e/o di esibizione del green pass, nonché il bilanciamento tra il diritto alla autodeterminazione terapeutica e la libertà di iniziativa economica (art. 41 Cost.).

In estrema sintesi, in assenza di diversi accordi/provvedimenti, il possesso dei requisiti richiesti per il rilascio del green pass (avvenuta vaccinazione, guarigione dal Covid-19 o tampone negativo), e quindi anche la legittimità delle possibili restrizioni contrattuali riconducibili al rifiuto opposto dal lavoratore (partendo dal negato accesso ai servizi di ristorazione, per arrivare sino all'estremo del rifiuto della prestazione lavorativa), presuppongono, quanto meno:

1. una specifica indicazione del medico competente che, nell'ambito del processo di applicazione in azienda dei Protocolli nazionali, qualifichi questi elementi, nel contesto

[63] Tribunale di Verona Sez. Lav., 24 maggio 2021, n. 446- La Oss rifiuta il vaccino. Legittima l'aspettativa non retribuita – studio legale avv. paola maddalena ferrari (studiolegaleferrari.it)

[64] Bollettino Adapt n. 29/2021 sez. *Labour Lawyers*: Tribunale di Pavia, ordinanza 20 luglio 2021
In caso di mancata vaccinazione, il datore di lavoro può sospendere, senza riconoscere la retribuzione, l'operatore socio-assistenziale dal servizio o, in alternativa, consentire il godimento delle ferie arretrate - Bollettino Adapt

aziendale di riferimento, quale misura "volta al contenimento del rischio di contagio da virus SARS-CoV-2/COVID-19 (Protocollo nazionale del 6 aprile 2021)

2. che tale determinazione sia oggetto della procedura di confronto nell'ambito del "Comitato per l'applicazione e la verifica delle regole contenute nel presente Protocollo di regolamentazione" (Protocollo condiviso di aggiornamento delle misure per il contrasto e il contenimento della diffusione del virus SARS-CoV-2/COVID-19 negli ambienti di lavoro del 6 aprile 2021). Tale confronto non richiede l'accordo, pur essendo auspicabile.

Una nota a latere merita il tema dell'obbligatorietà dell'esibizione del Green pass quale condizione per l'accesso alle mense aziendali, nelle FAQ pubblicate dal Governo il 14 agosto 2021[65] la conferma dell'obbligo sia per i dipendenti pubblici sia per i privati. Tale precisazione smentisce quanto deciso qualche giorno prima dal ministero dell'interno in relazione al proprio personale dipendente, difatti nella circolare del 5 agosto scorso, in cui il Viminale escludeva l'obbligo di esibizione del Green pass per usufruire della mensa interna.

Si riporta di seguito, la risposta fornita al quesito circa la necessità di esibire il Green pass da parte dei dipendenti per la consumazione al tavolo nelle mense aziendali, o comunque in tutti i locali adibiti alla somministrazione di servizi di ristorazione: "Sì, per la consumazione al tavolo al chiuso i lavoratori possono accedere nella mensa aziendale o nei locali adibiti alla somministrazione di servizi di ristorazione ai dipendenti, solo se muniti di Green pass, analogamente a quanto avviene nei ristoranti. A tal fine, i gestori dei predetti servizi sono tenuti a verificare il Green pass con le modalità indicate dal decreto del Presidente del Consiglio dei ministri 17 giugno 2021[66]"

Confindustria ha pubblicato una nota di aggiornamento il 18 agosto 2021[67] , nella quale presenta le proprie soluzioni ai principali interrogativi emersi negli operatori del settore, in particolare per la nostra trattazione, gli interrogativi su come devono inquadrarsi i rapporti tra datore di lavoro e fornitore del servizio mensa relativamente all'obbligo di verifica del Green pass, anche e soprattutto sul versante privacy. In tema, il punto 5.12 della nota di Confindustria risponde come segue: "In termini generali, il punto è stato affrontato sul piano normativo dal DPCM del 17 giugno 2021, che in sostanza "limita" le verifiche sul possesso del Green pass alle generalità del possessore e alla autenticità e alla corrente validità del medesimo, al momento della verifica. Per queste ragioni il "sistema Green pass" non pone particolari problematiche sul piano della tutela della riservatezza dei

[65] COVID-19 – Domande frequenti sulle misure adottate dal Governo | www.governo.it

[66] GU Serie Generale n.143 del 17-06-2021; link: *decreto del Presidente del Consiglio dei ministri 17 giugno 2021*

[67] Confindustria link alla nota di aggiornamento del 18 agosto 2021

dati personali. Nello specifico, la FAQ chiarisce l'obbligo di esibizione tra lavoratore dipendente e gestore della mensa, per cui il datore di lavoro resta tendenzialmente soggetto terzo, non interessato direttamente alla conoscenza del possesso di un green pass valido. Egli potrebbe venire a conoscenza del rifiuto del gestore e dedurne il motivo, che comunque resta generico (mancato possesso del green pass, green pass scaduto) e non consente di fare riferimento ai presupposti che hanno consentito il rilascio del Green pass".

Dunque, titolare del trattamento, considerato il DPCM 17 giugno 2021 e le FAQ del Governo risulta essere, almeno in termini generali, il gestore della mensa. Al gestore della mensa viene attribuito l'obbligo specifico di esercitare l'attività di controllo del Green pass, venendosi quindi a creare un rapporto giuridico diretto con il dipendente rispetto al quale il datore di lavoro resta soggetto terzo ed estraneo. Alla data non si riportano chiarimenti del Garante della protezione dei dati personali, sebbene le critiche e le perplessità sollevate dai settori coinvolti e le Parti sociali, le necessarie azioni di adeguamento sono state necessariamente intraprese.

6.1. Obbligo, facoltà o dovere libero

Si riporta di seguito una problematica interessante ed una dissertazione rispetto ad una possibile qualificazione di un dovere o, diversamente, di una facoltà per il datore di lavoro di chiedere la certificazione anche al lavoratore e, specularmente, l'obbligo o la facoltà di quest'ultimo di munirsene per rendere la prestazione di lavoro[68] "…L'art. 3 del D.L. n. 105/2021 non sembrerebbe porre un obbligo generalizzato del possesso del Green Pass; piuttosto, subordina l'ingresso in alcuni luoghi al possesso di questo. Tant'è che non tutti i settori sono interessati dalla norma. In questa prospettiva, il cittadino-lavoratore non è destinatario dell'obbligo di dotarsi del Green Pass ma viene limitato nelle scelte e nelle azioni, essendo previsto che per accedere, a qualunque titolo, in determinati spazi è necessario accertare il possesso della certificazione. Questa "scelta" può essere accostata a quello che la dottrina privatistica definisce «dovere libero», ossia «un comportamento a cui il soggetto è tenuto per realizzare un interesse suo proprio; è un evento da realizzare per poter esercitare un diritto»; infatti, «l'inadempimento dell'onere si traduce nell'impossibilità per il titolare di soddisfare il suo interesse». Seguendo questa impostazione, ne deriva che la certificazione verde è un onere al quale il cittadino-lavoratore deve ottemperare per esercitare i suoi diritti in quei contesti individuati dalla norma. Correlato a questo onere si riscontra il dovere del datore di lavoro – o del suo preposto – di verificare che vi sia il presupposto affinché il lavoratore possa esercitare i suoi diritti e i suoi doveri negli ambienti di lavoro. Un dovere che se violato, la legge sanziona con pene pecuniarie, prevedendo

[68] Benincasa G. - Piglialarmi G., *Green Pass e rapporti di lavoro*, WP Salus n. 7/2021 pag. 6, 7.

anche la sospensione temporanea dell'attività d'impresa. Il profilo sanzionatorio rafforza, dunque, l'idea che si tratti di un dovere anziché di una facoltà del datore di lavoro…"

6.2.Green Pass e tutela della privacy

La verifica del possesso del Green Pass imposta dall' art.13, del D.P.C.M. del 17 giugno 2021 e disciplinata dall' art.9, comma 10, del D.L.n.52/2021, comportando la consultazione di dati personali di una persona fisica, ha impatto sull' ambito di applicazione Regolamento UE 2016/679, ponendo all' attenzione questioni relative al trattamento dei dati personali. Per consentire l'accesso ai luoghi di lavoro per cui è previsto l'obbligo del Green Pass e/o per fruire di determinati servizi indicati dalla legge, l'attività di verifica può essere delegata con atto formale dal titolare di imprese o enti ad un soggetto incaricato. Tale soggetto coprirà il ruolo di soggetto autorizzato al trattamento dei dati. Il titolare dovrà fornire istruzioni sul trattamento, sui profili della sicurezza del trattamento e tutte le necessarie informazioni. Questi dovrà spiegare di quali dati sia possibile la verifica, verifica da condurre esclusivamente tramite la App ufficiale predisposta dal Ministero per la Salute, e ribadire la necessità di non raccogliere dati dall' intestatario in accordo al principio di minimizzazione. La delega dovrà essere in primis nominativa ed in secondo luogo completa di tutte le informazioni sulle modalità di effettuazione delle operazioni di verifica e consultazione.

Il Garante per la privacy è intervenuto più volte, con particolare riferimento alla disciplina della certificazione verde delineata dal D.L. n. 52/2021, dapprima con il Provvedimento di avvertimento in merito ai trattamenti effettuati relativamente alla certificazione verde per Covid-19 prevista dal D.L. 22 aprile 2021 n. 52 stesso e da ultimo ribadendo l' utilizzo del Green Pass diverso dalle ipotesi previste dalla legge non possano ritenersi ammissibili in quanto non garantirebbero il rispetto del principio di esattezza dei dati trattati. Tale principio risulta oggi garantito nei casi individuati dal citato D.L. n. 52/2021 grazie all' utilizzo della piattaforma DGC (Piattaforma Nazionale Digital Green Certificate) che possiede le caratteristiche per realizzare un concreto e legittimo obiettivo di interesse pubblico idoneo a legittimare il relativo trattamento dati[69].

[69] Parere sul DPCM di attuazione della piattaforma nazionale DGC per... - Garante Privacy

CONCLUSIONI

È opinione diffusa che nell'ultimo ventennio si sia verificato un passaggio epocale destinato a trasformare profondamente la società nel suo complesso. Si è infatti estesa e consolidata la convergenza e l'interdipendenza delle tecnologie informatiche, elettroniche e di telecomunicazione, il che ha determinato una svolta significativa nell' impiego delle tecnologie stesse. Si sono realizzati nuovi prodotti e servizi, classificabili nell' area della "multimedialità interattiva" e destinati non più solo alle imprese e agli organismi pubblici, ma a tutti gli individui, in quanto fortemente interessati alle nuove possibili forme di partecipazione e comunicazione sociale. Così ridefinite le tecnologie dell'informazione e della comunicazione si sono affermate come strumento fondamentale per tutti i soggetti sociali, sia pubblici che privati e per ogni tipo di riforma, organizzativa, procedurale o produttiva.

In questa prospettiva si è evidenziato il ruolo strategico delle infrastrutture avanzate di comunicazione: il "sistema nervoso" della nuova società globale dell'informazione, le cosiddette autostrade informatiche, le reti di comunicazione, nonché i servizi di base e l'accesso elettronico alle informazioni, le applicazioni e le informazioni gestite attraverso le reti stesse. In tale contesto, i diritti della persona sono esposti a ben maggiori pericoli in una società dove l'informatica, la telematica e la multimedialità hanno cancellato il tempo e lo spazio nello scambio di informazioni, ciò anche all' insaputa o contro la volontà dell'interessato.

Tale pericolo cresce con il perfezionarsi dei sistemi, la potenzialità lesiva della raccolta e del trattamento dati è di per sé enorme, anche se non va assolutizzata. Il concetto di privacy assume un duplice profilo, che i giuristi d' oltreoceano hanno inizialmente qualificato come "*disclosural privacy*", accentuando l'attenzione sulla diffusione e la rilevazione di dati notizie riservate, o come "*informational privacy*", riferendosi alla potenzialità lesiva della raccolta e del trattamento dei dati.
La rivoluzione indotta dal GDPR e le sue novità come presentate nel corso di questo studio, hanno in effetti coniugato entrambi gli aspetti. Ai poteri riconosciuti all' interessato in merito alla tutela dell'*Informational privacy*, si è affiancata la tutela risarcitoria della *disclosural privacy*.

Nella sostanza emerge, dallo studio delle fonti, che si è aperta una nuova stagione nella protezione dei dati personali, in cui la regolazione unitaria a livello europeo assume un valore decisivo, laddove l'intervento del legislatore interno è destinato ad essere, se non marginale, quanto meno integrativo e complementare rispetto a quello sovranazionale. Ciò è tanto più vero per il fatto che esso sarà tenuto

ad ispirarsi, nel solco dell'impostazione del GDPR, ad una regolazione leggera, che conservi ampio margine alla responsabilizzazione del singolo titolare, fin dalla fase di progettazione del trattamento, quale principio cardine dell'intero quadro normativo.

La centralità del principio di *accountability*, che si sostanzia alla valorizzazione dell'assunzione di responsabilità da parte dei singoli titolari in particolare nella valutazione del livello di rischio dei trattamenti e della conseguente necessità di adottare gli adempimenti previsti normativi nonché dell'adeguatezza delle misure di protezione, segna un profondo cambiamento culturale rispetto all'imposizione della normativa precedente. Si è passati ad una prima regolazione fondata sulla visione proprietaria dei dati, in cui le autorizzazioni e in più generale i controlli preventivi del Garante rivestivano un peso rilevante, fino ad una legislazione che ha progressivamente lasciato all'Autorità pubblica un ruolo di mero soggetto regolatore, a fronte di una valorizzazione, sotto il profilo sostanziale, dell'assunzione di responsabilità del singolo titolare del trattamento, laddove l'intervento del Garante è pensato in ottica di controllo e di eventuale sanzione a posteriori nel caso in cui si sia verificato un abuso del margine di autovalutazione lasciato ai singoli.

La privacy si conferma, così, come un diritto dal carattere fortemente dinamico che richiede un adattamento al mutare delle esigenze della società e della tecnologia.

In un contesto complesso come l'emergenza sanitaria da COVID-19, caratterizzata dalla strenua lotta per la mitigazione della pandemia e la gestione dell'emergenza, suscettibile di alterare il sistema delle garanzie democratiche come indicato dal Presidente dell'Autorità Garante per la Protezione dei Dati Personali[70], la disciplina della privacy si è quindi rilevata uno strumento prezioso.

Abbiamo osservato nel corso della trattazione come il valore di questo straordinario diritto si sia manifestato come requisito ad un tempo di libertà e di democrazia assicurando alla società il giusto equilibrio tra privato e pubblico, tra diritti e solidarietà, ponendo la tecnica al servizio dell'uomo e non viceversa.

La stagione della condizione pandemica ci ha insegnato a convivere con la limitazione dei diritti ed è stata un catalizzatore rilevando la profonda interrelazione tra la nostra vita ed il digitale. Nel continuo bilanciamento tra diritto alla salute e diritto alla protezione dati, in ragione della situazione emergenziale, abbiamo appreso, tutti ed a vari livelli, che la compressione dei diritti e delle libertà delle persone possono essere limitati soltanto nella misura del cosiddetto "strettamente

[70] Relazione Annuale 2020 Garante Privacy

indispensabile" e devono essere periodicamente valutati per verificare che le limitazioni imposte siano sempre necessarie e soprattutto proporzionali rispetto alla situazione emergenziale stessa.

In questo contesto la protezione dati dei lavoratori ha assunto una funzione significativa in considerazione del fatto che i lavoratori rappresentano una categoria vulnerabile. Infatti, sono parte di un rapporto contrattuale con una controparte che assume una posizione più forte in grado di condizionare anche la loro volontà. Tale differenza di potere contrattuale potrebbe difatti impedire al lavoratore di compiere le proprie scelte in modo volontario ed autonomo.

In riferimento ai controlli dei lavoratori effettuati sul luogo di lavoro e finalizzati a prevenire il contagio da COVID-19 il criterio guida, indicato dall' Autorità Garante della protezione dati, nella valutazione della legittimità di tali controlli è quello per cui il trattamento dei dati particolari è lecito in caso di necessità di sanità pubblica alla luce di una previsione normativa che individui l'ambito del trattamento e le relative garanzie. Inoltre, l'esigenza di tutelare i lavoratori dal rischio del contagio deve essere contenuta dall'introduzione di misure finalizzate a prevenire tali rischi e garantire anche la protezione dei dati personali.

Nell' intrigata produzione normativa emergenziale, comunque sempre affiancata da interventi ad hoc dell'Autorità Garante per la protezione dei dati personali, attraverso chiarimenti, pareri e FAQ in riferimento ad aspetti nuovi che risultavano emergere, caso emblematico della normativa emergenziale risulta essere la norma complessa e contraddittoria per l'introduzione del Green Pass al lavoro[71], nel settore dell'istruzione e della sanità.

Si riscontrano difatti prescrizioni diverse per clienti ed addetti degli stessi servizi ed attività. Complessità e contraddittorietà della normativa sul Green Pass che, sottolinea Fondazione Studi Consulenti del Lavoro[72], nella sua analisi, si è forzatamente riflessa nel dibattito sull' obbligatorietà della vaccinazione nei luoghi di lavoro nonché sul documento richiesto per accedere a servizi ed attività. Nei settori in cui vige l' obbligo del Green Pass per gli "addetti ai lavori", le incoerenze non sono mancate, ad esempio, mentre al personale scolastico è richiesta la certificazione verde e, in caso di violazione, la sanzione prevede la sospensione del rapporto di lavoro senza retribuzione dopo il quinto giorno di assenza per mancanza del Green Pass, per gli alunni, fino alle superiori, non sussiste alcun obbligo, o ancora nella ristorazione, per cui, come noto, l' obbligo esiste da tempo, per i clienti che pranzano al chiuso, ma non per camerieri, cuochi, responsabili di sala al lavoro.

[71] SEGHEZZI F. *Servono regole nazionali per mettere ordine nel caos del green pass al lavoro* Bollettino ADAPT n. 29 30 agosto 2021
[72] Consulenti del Lavoro - Green Pass e lavoro: norme disomogenee

Lo studio evidenzia come i datori di lavoro si siano dovuti misurare, durante le varie fasi della pandemia con l'introduzione di misure per il contenimento dei contagi, finalizzate alla protezione dei dipendenti pur mantenendo alta la capacità operativa aziendale. In questo scenario la tutela della privacy del dipendente ha dovuto ricercare punti di equilibrio non facili rispetto alla sicurezza, alla salute dei dipendenti stessi e alla necessità di garantire la continuità operativa. Si sono riportate allo scopo le tabelle sinottiche realizzate da Bird&Bird[73], in riferimento alla nostra realtà nazionale con vincoli ed obblighi per un datore di lavoro verso i propri dipendenti, le altre categorie contrattuali ed i visitatori nonché le linee guida da rispettare per riaprire e mantenere gli uffici in sicurezza.

L' esplosione della pandemia ha determinato il massiccio ricorso allo smart working nella sua modalità semplificata sempre raccomandato quale misura di contenimento principe per i contagi dal legislatore ed altresì raccomandato dal susseguirsi degli aggiornamenti dei Protocolli tra le parti sociali. Tuttavia, cambiando le condizioni logistiche e strumentali della prestazione lavorativa occorre tener conto che muta il contesto in cui deve garantirsi la protezione dei dati, pertanto l'improvvisazione iniziale deve ora dar spazio alle regole. Infatti, il distanziamento sociale imposto dalla pandemia ha portato i datori di lavoro a utilizzare sempre di più il sistema di smart working ed a farlo in modo repentino, spesso senza preventiva adeguata organizzazione del sistema e senza che gli stessi lavoratori fossero adeguatamente formati su tale modalità. Come ricordato dal Presidente dell'Autorità l'uso di tale sistema non può essere un modo per monitorare e controllare lo svolgimento dell'attività lavorativa del dipendente né un modo per controllare dove quest'ultimo si trovi. Al lavoratore in smart working deve essere riconosciuto il diritto alla disconnessione, cioè ad avere tempi e spazi necessari per la propria vita privata.

Come si può notare, le misure poste in essere ai fini di prospettiva prevenzione del contagio da COVID-19 hanno comportato e comportano una serie di oneri e responsabilità, destinati ad assorbire le imprese in svariati ambiti, non solo quello economico.

Consistenti, sono, infatti, gli adempimenti che gravano sul datore di lavoro, tra cui vanno ricompresi anche quelli conseguenti all'applicazione della disciplina in materia di protezione dei dati personali.

Guardando al futuro post pandemico è importante sottolineare le sfide che molte aziende si troveranno a fronteggiare con un aumento sostanziale del lavoro da remoto. Molti lavoratori potranno scegliere di lavorare in maniera permanente da remoto ed altri con prevalenza del lavoro agile o da remoto. Abbiamo visto anche nei casi di studio come le realtà organizzative si stiano orientando verso queste modalità riadattando alcuni processi o limitando lo smart working ad alcune funzioni. Questo

[73] data-protection_covid-19-v03.pdf (twobirds.com)

avrà un impatto soprattutto sul disegno dei nuovi uffici del futuro con una forte probabilità di un ridisegno degli spazi con posti di lavoro (scrivanie) in modo da accomodare il rientro delle persone in maniera più o meno sporadica e anche con molti spazi negli uffici dedicati a spazi per incontri, sale riunioni, sale per video conferenze con forte contenuto digitale. Il ridisegno degli spazi implicherà una maggiore attenzione agli aspetti ergonomici e di salute come pure alla salvaguardia della "privacy del lavoratore".

Molti studi hanno evidenziato come in situazioni normali il lavoro agile può incrementare la produttività insieme ad un migliore bilanciamento tra vita privata e vita professionale. Ciononostante, in situazioni di crisi queste condizioni si possono deteriorare anche in ragione di una mancanza di organizzazione della vita famigliare, mancanza di spazi idonei e disponibilità di strumenti IT. I datori di lavoro debbono quindi tenere in conto la qualità del lavoro in generale ed in particolare al benessere ed alla sicurezza del lavoratore.

Finita la crisi ed in una situazione in cui il lavoro agile non è più un elemento primario come risposta alla crisi pandemica, i datori di lavoro debbono operare scelte strategiche nell'organizzazione del lavoro tenendo in conto le preferenze dei lavoratori ma anche evitare effetti negativi sulla produttività, bilanciamento lavoro-vita personale ed anche rischi psico-sociologici.

Quindi, sebbene la pandemia da COVID-19 ha causato danni considerevoli all'economia in generale ed alle persone in particolare, la riorganizzazione del lavoro post-pandemico rappresenta un'ottima opportunità per ridefinire anche la vita lavorativa facendo leva su un uso concreto del lavoro agile pur mitigando i rischi legati al benessere, salute e privacy del lavoratore.

.

BIBLIOGRAFIA

BARILE P. - CHELI E. *Domicilio (libertà di),* in *Enciclopedia del Diritto, XIII*, 1964, pagg. 859-870.

BELLAVISTA A, *I poteri dell'imprenditore e la privacy del lavoratore*, in *Dir. Lav*., 2002, 3, pp.153 ss.;

ID., *Privacy e protezione dei dati personali nel rapporto di lavoro subordinato: problemi e prospettive*, in *Vita not*., 1995, 3, pp.1589 ss.;

ID., *Il controllo sui lavoratori, Giappichelli*, Torino, 1995.

BENINCASA G. - PIGLIALARMI G., *Green Pass e rapporti di lavoro,* WP Salus n. 7/2021

BUTERA F. *Le condizioni organizzative e professionali dello smart working dopo l'emergenza: progettare lavoro ubiquo fatto di ruoli aperti e di professioni a banda larga* in Stud. Org., n.1 2020, pp. 141.165

BUTTARELLI G. - *Banche dati e tutela della riservatezza*, Milano 1997, pag. 8 ss.

CARINCI M.T., *Il controllo a distanza dei lavoratori dopo il "Jobs Act" (art. 23, D.lgs. 151/2015) spunti per un dibattito, in Labour and Law Issues, 2016*, 1, p. V.

CARTA C., *I limiti al potere di controllo sui lavoratori nell'uso di internet e dei servizi di comunicazione elettronica: per un diritto alla moderazione*, in *Labor*, 2018, 2, p. 174;

CASILLO R., *La dignità nel rapporto di lavoro, in RDC,* 2008, n. 5, p.593

COSTANTINI F., *Il Regolamento (UE) 679/2016 sulla protezione dei dati personali*, in *Lav. Giur*., 2018, p.553.

CUFFARO V., RICCIUTO V., ZENO-ZENCOVICH V. *Trattamento dei dati e tutela della persona,* Milano, 1998, pag. 51 ss.

DAGNINO E., MENEGOTTO M., PELUSI M. L., TIRABOSCHI M. *Guida pratica al lavoro agile* ADAPT University Press, 2020

D'ARCANGELO L., *Contact tracing e protezione dei dati nella fase 2 dell'epidemia da COVID-19 (anche nel rapporto di lavoro),* in *Giustiziacivile.com, n. 3 (speciale),* p. 6

DALLACASA M., *controlli su strumenti informatici dopo la sentenza Barbulescu del 207 della Cedu*, in *Lav. Giur.*, 2018, 5, pp437 ss.

DE MASI D., *Smart Working. La rivoluzione del lavoro intelligente*, Marsilio Editore 2020

INGRAO A., *Il controllo a distanza effettuato mediante Social network, in Labour & Law Issues*, 2016, 1, p. 105.

IASELLI M., *Manuale Operativo del D.P.O (Data Protection Officer)*, Maggioli Editore, 2018

ID., *La gestione della privacy in periodi di emergenza*, EPC Editore, 2020

JELINEK A., *Linee Guida 04/2020 sull'uso dei dati di localizzazione e degli strumenti per il tracciamento dei contatti nel contesto dell'emergenza legata al COVID-19*, EDPB, 21 aprile 2020

LAMBERTUCCI P., *svolgimento del rapporto di lavoro e tutela dei dati personali*, in CARINCI F., DE LUCA TAMAJO R., TOSI P., TREU T. (a cura di), *La tutela della privacy del lavoratore*, in *Quad. dir. Lav. rel. ind.*, 2000, 24, pp. 61 ss.

LOCORATOLO B., *Il trattamento dei dati personali e la privacy*, Gruppo Editoriale Simone, 2021

MARTONE M. (a cura di), *Il Lavoro da Remoto – Per una riforma dello smart working oltre l'emergenza* Tribuna d'Autore, 2020.

PERRONE F., *La tutela della privacy sul luogo di lavoro: il rinnovato dialogo tra Corte Europea dei Diritti dell'Uomo e giurisdizione nazionale la sentenza Barbulescu 2, in Labor*, 2018, 3, pp. 283 ss;

PESSI R., *Lezioni di diritto del lavoro*, Giappichelli Editore 2018.

PETRINI C. ed altri, *Protezione dei dati personali nell'emergenza COVID-19*, Gr. di lav. Bioetica COVID-19, Rapporto ISS COVID-19 n. 42/2020

PIGNI G. *Il lavoro da remoto come misura necessaria per affrontare l'emergenza Covid-19 – Le scelte dei governi in Europa e negli Usa*, WP n. 14, ADAPT University Press 2020

PIZZOFERRATO A., *Gli effetti del GDPR sulla disciplina del trattamento aziendale dei dati del lavoratore, in Argomenti Dir. Lav*., 2018, n. 4-5 p- 1037.

PRETEROTI A., *Lavoro e previdenza*, in M. BIANCA, F.D. BUSNELLI (a cura di), *La protezione dei dati personali: commentario al d.lgs. 30 giugno 2003, n. 196,* Cedam Padova *2007*, p. 1467;

SANTORO-PASSARELLI G., *Il lavoro autonomo non imprenditoriale, il lavoro agile e il telelavoro*, in *Riv. it. Dir. Lav*. 2017, 3, p.383.

SEGHEZZI F., *Servono regole nazionali per mettere ordine nel caos del green pass al lavoro* Bollettino ADAPT n. 29 agosto, 2021.

SCAGLIARINI S. (a cura di), *Il "nuovo" codice in materia di protezione dei dati personali – La normativa italiana dopo il d.lgs. n. 101/2018* Giappichelli Editore (collana fondazione M. Biagi) – Torino 2019

STANZIONE P., *Tecnica, Protezione dei dati e nuove vulnerabilità*, Rel. Ann. Presidente P. Stanzione GPDP, Roma 2021