



**MARZO 2020**

**Autore:** MULTIBUSINESS SRL – “GarantePrivacyItalia”

**Categoria:** Economia, lavoro e Pubblica Amministrazione

**Sotto-Categoria:** Tutela e Protezione Dati Personali - “Privacy”

**Norme e prassi:** *Regolamento UE 679/2016 – D.Lgs. 196/2003 e ss.mm.ii (D.Lgs. 101/2018)*  
*Statuto dei Lavoratori L. 300/1970 – DPCM relativi al COVID19*

**Notizia del  
giorno:**

**CORONAVIRUS: GARANTE PRIVACY, NO A INIZIATIVE  
"FAI DA TE" NELLA RACCOLTA DEI DATI**

Sia i soggetti pubblici che i soggetti privati devono attenersi alle indicazioni del Ministero della salute e delle istituzioni competenti in materia, relativamente a tutte le attività mirate al contenimento del COVID19 (più comunemente conosciuto con il termine “Coronavirus”)

**Indice Rassegna:**

- ® IL CORONAVIRUS INTIMORISCE I DATORI DI LAVORO: ma la “privacy” di dipendenti e visitatori va comunque rispettata
- ® SMART WORKING E CONTROLLI SUI LAVORATORI
- ® CORONAVIRUS E PRIVACY: Possibile la geolocalizzazione, ma compatibile con i valori democratici
  - Allegato 1\_ Comunicato del Garante Privacy del 2 Marzo 2020
  - Allegato 2\_ Direttiva n. 1/2020 Ministro per la Pubblica Amministrazione del 26 Febbraio 2020

## **IL CORONAVIRUS INTIMORISCE I DATORI DI LAVORO: ma la "privacy" di dipendenti e visitatori va comunque rispettata**

Il Coronavirus fa paura, ma la normativa d'urgenza adottata nelle ultime settimane **non permette** di violare la privacy di visitatori, utenti e dipendenti.

Sia i soggetti pubblici e che i soggetti privati **non possono** richiedere ai visitatori e/o agli utenti informazioni circa la presenza di sintomi da CORONAVIRUS e notizie sugli ultimi spostamenti, come misura di prevenzione dal contagio. Di contro, non è lecito acquisire un'autodichiarazione dai dipendenti in ordine all'assenza di sintomi influenzali (anche dei loro contatti più stretti, quali familiari), nonché vicende relative alla sfera privata.



Coronavirus: Garante Privacy, no a iniziat raccolta dei dati Soggetti pubblici e privat alle indicazioni del Ministero della salute e competenti

Questo è **quanto ha chiarito il Garante per protezione dei dati personali** con comunicato del 2 Marzo 2020 (che si allega), evidenziando nel contempo che la finalità di prevenzione dalla diffusione del Coronavirus va svolta da soggetti che **istituzionalmente esercitano queste funzioni** in modo qualificato, e che quindi possono raccogliere informazioni relative ai sintomi tipici del Coronavirus, nonché in merito ai recenti spostamenti degli stessi (a titolo esemplificativo operatori sanitari, protezione civile, ecc). È stato previsto che chiunque negli ultimi 14 gg abbia soggiornato nelle zone a rischio epidemiologico, debba comunicarlo all'Azienda Sanitaria Territoriale, anche tramite il medico di base.

Con particolare riferimento alle informazioni richieste dai datori di lavoro ai propri dipendenti, si rammenta che, ai sensi dell'art. 9 del Regolamento UE 2016/679, i dati relativi alla salute dei lavoratori possono essere trattati dai Titolari del trattamento (quindi dai datori di lavoro), **solo** nel caso in cui il trattamento sia necessario per assolvere gli obblighi ed esercitare i diritti specifici del Titolare stesso o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e (in sostanza non è questa la fattispecie).

### **Detto quanto sopra, va tuttavia ricordato che vige l'obbligo:**

- per i lavoratori di segnalare ai datori di lavoro situazioni di pericolo per la salute e la sicurezza sui luoghi di lavoro;
- per i datori di lavoro comunicare agli organi preposti l'eventuale variazione del rischio "biologico" derivante dal CORONAVIRUS per la salute sul posto di lavoro, ed effettuare gli altri adempimenti connessi alla sorveglianza sanitaria sui lavoratori (ad esempio sottoponendo ad una visita straordinaria i lavoratori più esposti).

Inoltre, il **Garante ha evidenziato** che, di recente, il Ministro per la Pubblica Amministrazione, ha fornito indicazioni operative circa l'obbligo per il dipendente pubblico e per chi opera a vario titolo presso la P.A. (ovvero di segnalare all'amministrazione di provenire da un'area a rischio).

Qualora nel corso dell'attività lavorativa, il dipendente che svolge mansioni a contatto con il pubblico (URP, prestazioni allo sportello, reception, ecc), venga in relazione con un caso sospetto di CORONAVIRUS, lo stesso (o tramite il datore), è tenuto a comunicare la circostanza ai servizi sanitari competenti e ad attenersi alle indicazioni fornite.

Ministro per la  
Pubblica Amministrazione

\* In relazione alle P.A. si segnala che, in data 26 Febbraio 2020, il Ministro per la Pubblica Amministrazione ha emanato la Direttiva n. 1/2020 (che si allega), la quale fornisce indirizzi operativi di carattere anche precauzionale per le P.A., che devono, tra l'altro, assicurare l'applicazione delle misure alle società a controllo pubblico ed agli enti vigilati.

Per gli uffici adibiti al ricevimento del pubblico o in generale nei locali frequentati da personale esterno, la direttiva raccomanda di:

- evitare il sovraffollamento anche attraverso lo scaglionamento degli accessi;
- assicurarne la frequente aerazione;
- effettuare un'accurata pulizia e disinfezione delle superfici ed ambienti;
- mantenere un'adeguata distanza con l'utenza.

Nei locali, aperti al pubblico e non, dovranno poi essere rese disponibili strumenti di facile utilizzo per l'igiene e la pulizia della cute, quali ad esempio dispensatori di disinfettante o antisettico per le mani, salviette asciugamani monouso, nonché, qualora l'autorità sanitaria lo prescriva, guanti e mascherine per specifiche attività lavorative.

È a tali misure di prevenzione che si riferisce il Garante quando nel suo comunicato parla di misure di prevenzione generale alle quali ci si deve attenere per assicurare l'accesso dei visitatori ai locali aperti al pubblico nel rispetto delle disposizioni d'urgenza adottate.

Alla luce di quanto sopra il Garante conclude invitando tutti i Titolari ad attenersi scrupolosamente alle indicazioni fornite dal Ministero della salute e dalle istituzioni competenti per la prevenzione della diffusione del CORONAVIRUS, senza effettuare iniziative autonome che prevedano la raccolta di dati anche sulla salute di utenti e lavoratori che non siano normativamente previste o disposte dagli organi competenti.

## SMART WORKING E CONTROLLI SUI LAVORATORI

L'emergenza del CORONAVIRUS ha accelerato l'adozione del **lavoro agile**, ma le aziende (sia pubbliche che private) nonché le singole persone, potrebbero non essere pronte ad una corretta gestione (ad esempio sui controlli effettuati).

Il ricorso massiccio al lavoro agile (c.d. *Smart Working*) per far fronte all'emergenza causate dal CORONAVIRUS, può rivelarsi una grande opportunità per il mercato del lavoro. Le aziende e i lavoratori (sia pubblici che privati) possono scoprire i benefici derivanti da una forma di svolgimento della prestazione di lavoro che mette al centro del rapporto la fiducia, come leva per ottenere più produttività nonché più flessibilità nella gestione del tempo e dello spazio di lavoro.



Tuttavia questo strumento nasconde una **forte insidia**: i soggetti coinvolti potrebbero non essere pronti a gestire correttamente il cosiddetto Smart Working.

L'impreparazione che potrebbe emergere è la gestione dei controlli sul lavoratore. Ciascun datore di lavoro infatti ha il diritto (nonché il dovere) di svolgere controlli sul corretto svolgimento della prestazione dei propri dipendenti, a patto che siano rispettati i limiti fissati dagli articoli 2, 3 e 4 dello Statuto dei Lavoratori.

### Controlli vietati

- L'articolo 4 dello Statuto dei Lavoratori ha una particolare rilevanza in tema di lavoro agile, perché fissa un principio molto rigoroso, ovvero: "sono vietati l'installazione e l'uso di apparecchiature tecnologiche e sistemi in grado di controllare a distanza lo svolgimento dell'attività lavorativa del dipendente, a meno che il ricorso a questi apparecchi non sia prima concordato con un accordo sindacale o sia autorizzato dall'Ispettorato territoriale del lavoro".

La norma, nata nel 1970 (ovvero lo Statuto dei Lavoratori), è stata interpretata in maniera evolutiva dalla giurisprudenza (e soprattutto dagli orientamenti del Garante Privacy), finendo per comprendere anche gli strumenti di controllo digitale della prestazione (ad esempio sistemi di rilevazione della posizione, software che monitorano in maniera costante l'uso che viene fatto di internet, ecc). Si tratta, in sostanza, sempre e comunque di **forme di controllo vietate** in base ai principi dello Statuto.



I datori di lavoro non potranno usare i software aziendali, le webcam e le altre tecnologie digitali per capire se lo smart worker (ovvero il lavoratore) sia collegato al suo computer, se si trova in casa o se invece sta facendo altro, e/o per verificare quali siti internet utilizza (tale comportamento sarebbe illecito).

Il Jobs Act (D.Lgs 151/2015, articolo 23) ha aggiunto un elemento importante: i dati e le informazioni ottenuti tramite gli strumenti di controllo a distanza sono utilizzabili «ai fini del rapporto di lavoro» solo a condizione che sia stata data al lavoratore «adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dalla normativa sulla "privacy"». In sostanza significa che, anche se lo strumento di controllo a distanza è lecitamente installato, il datore di lavoro deve preventivamente informare il lavoratore agile sulla possibilità di eseguire controlli sulla sua prestazione.

### **I controlli ammessi**

Premesso quanto sopra, la domanda che si pone spontanea è: "C'è quindi un divieto assoluto di controllo? Assolutamente no, vediamo perché.

Se il datore di lavoro ha il fondato sospetto che il dipendente stia commettendo degli illeciti, può svolgere controlli mirati, anche a distanza, a patto che siano **proporzionati e non invasivi**, e che riguardino beni aziendali (il Pc fornito dal datore, la casella di posta aziendale, ecc), rispetto ai quali il dipendente non ha alcuna "aspettativa di segretezza" (va chiarito, "ex ante", che gli strumenti aziendali non possono essere usati per motivi personali, poichè potrebbero essere oggetto di indagini aziendali).

Nei confronti dello Smart Worker, va considerato un elemento aggiuntivo, che consiste nell'**accordo individuale di lavoro agile** (accordo che, durante l'emergenza del CORONAVIRUS **può anche non essere siglato**), può disciplinare le forme di esercizio del potere di controllo, per i periodi nei quali l'attività lavorativa viene svolta fuori dai locali aziendali, definendo anche le condotte che danno luogo all'applicazione di eventuali sanzioni disciplinari. \*Le parti potrebbero quindi stabilire specifiche forme di controllo, sempre restando dentro i limiti dell'articolo 4 dello Statuto dei lavoratori.

## **CORONAVIRUS E PRIVACY: Possibile la geolocalizzazione**



La geolocalizzazione (ad esempio il sistema GPS delle auto aziendali), quale misura di prevenzione del contagio da COVID-19, **è possibile**, ma rispettando alcune condizioni. Il trattamento DEVE: avere una base giuridica normativa, rispettare i principi di proporzionalità, garantire il diritto di difesa in via giudiziale.

Il tracciamento dei dispositivi elettronici in uso a singoli individui (ad esempio per verificare il rispetto della quarantena o dell'isolamento domiciliare), **è già stato attuato** in paesi terzi (*Taiwan, Cina e Israele*). Tracciare il percorso significa avere la possibilità di **individuare la "catena del contagio"**, accertando chi vi è entrato in contatto. Il "problema" è la compatibilità con il diritto alla "privacy" dell'uso della tecnologia.

Come affermato dal Presidente dell'EDPB (ovvero il Comitato Europeo per la Protezione dei Dati), la materia della geolocalizzazione merita un doppio approccio:

- All'art. 9, p. 2, lett. i), il GDPR detta una specifica base giuridica per perseguire **motivi di interesse pubblico nel settore della sanità pubblica**, quali la protezione da gravi minacce per la salute a carattere transfrontaliero, purchè siano previste misure appropriate e specifiche a tutela dell'interessato;
- In materia di geolocalizzazione bisogna aggiungere regole derivanti dalla "E-Privacy Directive", ovvero la Direttiva 2002/58/CE relativa al trattamento dei dati e alla tutela della vita privata nel settore delle comunicazioni elettroniche.

La Direttiva impone una gradualità dei trattamenti, dando priorità di uso di informazioni anonime (ad esempio utilizzando dati aggregati con l'eliminazione della possibilità di ricondurli ai dati nominativi), questo comporta a un **sostanziale lasciapassare**.

Realisticamente l'utilizzo del dato anonimo potrebbe non essere sufficiente o non utile allo scopo specifico, ragion per cui il presidente dell'EDPB fa appello alla "Direttiva E-privacy", incentivando legislazioni nazionali finalizzate a **introdurre misure** nell'interesse della sicurezza nazionale e salute pubblica (una **legislazione d'emergenza** è possibile alla condizione che non mini i principi costitutivi dello stato democratico).

La "privacy" non è un ostacolo, essa però disegna il perimetro delle scelte compatibili. Questo perimetro **ammette anche deviazioni eccezionali**, motivate però oltre che dalla **eccezionalità** del momento anche dalla capacità di bilanciare i diversi interessi.