# COVID-19
# BYE BYE DIRITTO ALLA PRIVACY?

Smart working, app per la telepresenza, geolocalizzazione tramite celle telefoniche e, da ultimo, il contact tracing, sono alcuni degli strumenti hi-tech scesi in campo per fronteggiare l'emergenza da Covid-19 ma che rischiano di avere un impatto significativo sulla privacy

di **Paola Gobbi**

Quella che stiamo vivendo in queste settimane è la prima epidemia dell'era digitale. L'iniziativa della Lombardia di utilizzare i dati anonimi sui flussi di mobilità aggregati offerti dai gestori telefonici a cui è seguita la proposta di adottare un sistema di contact tracing sul modello coreano ha scoperchiato un vaso di Pandora: come impiegare le nuove tecnologie per controllare la diffusione dell'epidemia nel rispetto del diritto alla privacy? Nella cornice del GDPR, il diritto alla riservatezza non nasce come un diritto assoluto e il trattamento dovrebbe essere considerato lecito, anche senza il consenso dell'interessato ai sensi degli artt. 6 e 9, se diretto a tutelare interessi vitali ovvero per motivi di rilevante interesse pubblico, tra i quali può rientrare anche il controllo di un'epidemia. Ma questo non significa che, durante l'emergenza, il diritto alla privacy sia sospeso. Come precisato dal Comitato Europeo per la protezione dei dati con provvedimento del 19 marzo, il trattamento dovrà sempre avvenire nel rispetto del principio di proporzionalità, minimizzazione e trasparenza. Secondo il Garante Privacy sarebbe possibile introdurre, in via legislativa, limitazioni al diritto alla riservatezza purché proporzionate, temporanee e graduali, per finalità di contenimento dell'epidemia ed entro limiti temporali ben precisi. Misure eccezionali sono già in vigore, per esempio, negli ambienti di lavoro con le opportune cautele: i dipendenti possono essere sottoposti a controlli di temperatura, ma solo previa informativa e il dato acquisito non può essere registrato; inoltre i datori di lavoro possono informare il personale sui casi di Covid-19, raccogliendo però solo i dati indispensabili. L'emergenza ha costretto - però - imprese e lavoratori a mettere in secondo piano la privacy da quando gli strumenti informatici sono divenuti alleati preziosi per poter lavorare in smart working. In fase di registrazione delle app, non sempre ci si sofferma sui consensi concessi al servizio, trascurando che il "prezzo" per l'utilizzo di tutte queste applicazioni sono i dati personali lasciati durante la navigazione.

Le aziende dovrebbero essere consapevoli che quando i loro dipendenti si collegano in videoconferenza con i colleghi questi servizi hanno accesso ai dati audio, video e geolocalizzazione di tutti gli utenti in comunicazione e a file condivisi (foto, documenti e risorse aziendali), tutti dati che potrebbero anche essere ceduti a terzi ed essere incrociati. Per questo diventa importante fornire un adeguato training digitale ai dipendenti, affinché siano resi edotti della possibilità di gestire le impostazioni della privacy, in modo da minimizzare la raccolta dei dati. Inoltre, attenzione a non farsi prendere dall'entusiasmo e dall'improvvisa accelerazione nel ricorso allo smart working, anche senza gli ordinari accordi, ed eccedere nel trattamento. Occorre ricordare - come ben fa anche il citato provvedimento del Comitato Europeo - che le deroghe al consenso previste dall'art. 9 del GDPR riguardano gli organi pubblici e la sanità e non il datore di lavoro che, conseguentemente, non potrà avvalersi di trattamenti di dati se non nei limiti della informativa e del consenso già in essere oltre che per le finalità indicate.

Del resto, la moderatezza e l'utilizzo consapevole degli strumenti di navigazione assumono un ruolo ancor più importante tenuto conto che, ai sensi dell'articolo 17 del GDPR, proprio nei casi come il presente (di emergenza sanitaria e trattamento dati per interesse pubblico) non si ha sempre diritto a ottenere la cancellazione immediata di tutti i dati trattati, prevalendo un interesse superiore a quello del singolo interessato. In conclusione, la riservatezza resta un diritto fondamentale che potrà subire solo limitazioni temporanee e strettamente legate alla tutela del diritto alla salute, per evitare possibili abusi. Tuttavia, anche in un contesto emergenziale, occorre sempre essere informati sui dati raccolti e il loro trattamento, mettendo in campo qualche accortezza quando si "dialoga" con le nuove tecnologie.

Avv. **Paola Gobbi** partner UNIOLEX Stucchi & Partners - www.uniolex.com