



## **Il difficile bilanciamento degli interessi in gioco tra privacy e dati sanitari al tempo del COVID 19**

*di Antonio Cordasco, Avvocato*

In un momento delicato sul fronte sanitario, in cui fronteggiare la pandemia ponendo in essere misure straordinarie al fine di tutelare la salute pubblica è l'interesse prioritario, il possibile utilizzo di strumenti informatici atti a tracciare e trattare dati sensibili dei singoli, pone il problema del bilanciamento tra privacy del singolo e interesse collettivo. La giusta misura potrebbe arrivare da una attenta lettura del GDPR.

\*

L'ormai noto Regolamento comunitario sulla protezione dei dati personali n. 2016/679 UE, più citato come GDPR, non prevede una base giuridica specifica per il trattamento dei dati personali effettuato in ambito sanitario, tantomeno dedica una disciplina specifica per le situazioni emergenziali come quella in cui ci troviamo oggi, laddove tali situazioni potrebbero richiedere la necessità di trattare i dati relativi alla salute con modalità che normalmente si porrebbero fuori dalla base giuridica determinata dal consenso dell'interessato, consenso che costituisce lo strumento giuridico generalmente posto alla base del trattamento.

In questo momento di emergenza, la disposizione che sembra più idoneo richiamare è l'art.9 del GDPR, laddove nel porre un divieto generale del trattamento di particolari categorie di dati personali, al comma 2 stabilisce una serie di eccezioni tra cui, di nostro interesse, sono quelle previste alla lett. h) – relative al trattamento necessario per finalità di medicina preventiva -, alla lett. i) – trattamento necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a

carattere transfrontaliero, 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- ed in parte alla lett. j) laddove si richiama il trattamento necessario alla ricerca scientifica.

La questione si è posta nell'ambito della discussione che sta coinvolgendo non solo gli operatori del diritto ma anche sanitari e ricercatori, ovvero sulla possibilità di prevedere tracciamenti e/o comunicazione di dati relativi alla salute di terzi al fine di consentire di controllare e prevenire lo sviluppo del virus COVID 19, sul modello utilizzato in Cina, in Corea ed in Israele. La metodologia si basa su due metodologie: rendere fruibili a terzi, autorità sanitarie o singoli cittadini le informazioni relative agli spostamenti delle persone, attraverso l'utilizzo di dati già registrati negli smartphone, presi attraverso le celle telefoniche o dalle coordinate GPS, informazioni che, veicolate su apposite App, possono consentire di conoscere ad esempio, se nelle nostre vicinanze ha transitato un soggetto positivo al COVID 19; rendere possibile controlli in tempo reale circa le proprie condizioni di salute – e dunque circa il rispetto di eventuali restrizioni personali alla libera circolazione -, mediante App che, attraverso l'uso dei dati sanitari, possano fornire informazioni sul nostro stato di salute.

Su tali utilizzi, si pongono dunque doverosamente diversi interrogativi, anche in relazione alla sorte di questi dati che certamente verrebbero immagazzinati.

Innanzitutto il problema del consenso, che sembrerebbe parzialmente risolto attraverso il ricorso all'art.9 del GDPR nella parte citata, ma che sconta il limite del trattamento esclusivamente da parte delle Autorità sanitarie, laddove la disposizione riporta che le per le finalità del 9.2.h, i dati “..sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza”. Ammesso che si trovasse la modalità di consentire a soggetti che non possiedono dette caratteristiche, ad esempio gli sviluppatori delle App piuttosto che i gestori telefonici o della rete, di trattare i dati relativi agli spostamenti o relativi al proprio stato di salute senza la base giuridica del consenso fornito dal singolo interessato, rimarrebbe comunque la necessità di porre in essere una norma ad hoc, che ponga non solo limiti temporali alla conservazione dei dati una volta finita la necessità dell'uso, ma anche delle regole precise circa la sicurezza dei sistemi informatici per prevenire al massimo episodi di data breach, ovvero di furto dei dati.

Il Garante italiano ed il Comitato Europeo sulla protezione dei dati personali, hanno già precisato che l'emergenza può legittimare limitazioni alla privacy, sempre che tali limitazioni siano adottate in ossequio al periodo di emergenza.

Su tale orme si pone l'art.41 del Decreto Legge n.14 del 2020 che all'art. 14, fornisce la base giuridica del trattamento dei dati sanitari nel contesto emergenziale, precisando che, nel rispetto dell'art. 9, c.2, lett. g), h) i) dell'art.10 del GDPR e dell'art. 2 sexies c 2, lett. t) e u) del D. Lgv. 196/2003, i soggetti operanti nel

Servizio Nazionale di Protezione Civile ed i soggetti attuatori di cui all'art.1 dell'ordinanza del Capo del Dip.to della Protezione Civile n.630 del 03.02.2020, nonché gli Uffici del Ministero della Salute e dell'Istituto Superiore di Sanità nonché tutte le strutture pubbliche e private che operano nell'ambito del Servizio Sanitario Nazionale e i soggetti deputati a monitorare ed a garantire l'esecuzione delle misure disposte ai sensi della normativa di carattere emergenziale, possono effettuare trattamenti, ivi inclusa la comunicazione tra loro dei dati personali anche relativi agli artt. 9 e 10 del GDPR che risultino necessari all'espletamento delle finzioni attribuite nell'ambito dell'emergenza determinata dal diffondersi del COVID 19.

Quel che si reputa dover sottolineare è la conseguenza nel caso in cui si voglia tracciare i movimenti di persone risultate positive al COVID19 per avvertire terzi che sono entrati in contatto.

Torna quindi la problematica sopra accennata della gestione dei dati quando escono dalla disponibilità dei soggetti autorizzati ad agire sulla base giuridica del GDPR come richiamato dall'art.14 del Decreto Legge n.14/2020. Ciò in quanto, anche a voler reputare ovvia la circostanza che il trattamento dei dati relativi all'ubicazione dovrebbero essere anonimizzati, entra in gioco anche il contesto normativo dettato dalla Direttiva 2002/58/CE, meglio nota come Direttiva ePrivacy, poi modificata dalla direttiva 2009/136/CE, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, sebbene si sia in attesa del Regolamento che la sostituisca.

Ovviamente, la riservatezza deve essere adeguatamente salvaguardata anche al fine di evitare che un modello basato su eccezioni necessitate dall'emergenza possa essere utilizzato in violazione dei principi posti a salvaguardia dei diritti inviolabili tutelati dalla Carta Costituzionale, salvaguardia che può ben essere attuata seguendo, attraverso una normativa statutale, di tipo provvisorio, che preveda l'utilizzo di tutte le metodologie già conosciute che consentono l'anonimizzazione dei dati che si reputa di dover trattare a seconda della finalità perseguita, sia di controllo diretto dell'epidemia sia di controllo indiretto, permettendo a chiunque di sapere se si è stati nel raggio di contatto di soggetti portatori del virus.

La necessità di una normativa di livello primario e statutale deriva anche dalla circostanza che nel corso di questa imprevedibile e sconosciuta emergenza sanitaria, sono stati attribuiti ulteriori ed ampi poteri alle Autorità Locali, anche in deroga alle decisioni prese sul piano nazionale, aumentando il rischio di compromettere la possibilità di esercitare le libertà fondamentali in sicurezza per ciò che riguarda quei dati che dovrebbero restare non tracciabili se non previa scelta dell'utente.

Sarebbe pertanto auspicabile che lo sviluppo di applicazioni informatiche, che si sono certamente rivelate utili al controllo di una epidemia che non solo è in atto su tutto il globo, ma di cui non sono ancora prevedibili gli sviluppi a livello scientifico ed epidemiologico, siano accompagnate dall'adozione di una normativa che, come detto, disciplini anche gli aspetti connessi all'utilizzo dei dati, aspetti di non secondaria importanza, soprattutto in riguardo alla possibilità che i sistemi possano essere oggetto di data

breach, anche in considerazione del periodo di conservazione che potrebbe essere lungo. Senza contare i rischi alla tutela dei dati immagazzinati sui singoli smartphone laddove la ripresa della libertà di movimento ci potrebbe portare a doverli esibire o doverne consentire il trattamento in Stati che disciplinano la materia diversamente dai Paesi dell'Unione Europea.