App Immuni

efficacia dello strumento, trasparenza delle informazioni, garanzie dei diritti fondamentali.

L'attesa della fase due si è accompagnata con diverse criticità e polemiche. Sicuramente molto scalpore ha riscosso il tema relativo alla predisposizione di un'app per il tracciamento dei contagi, soprattutto a fronte dell'ordinanza del Commissario Straordinario per l'emergenza con la quale, il 16 aprile, veniva stipulato il contratto di concessione gratuita della licenza d'uso sul software di *contact tracing* e di appalto di servizio gratuito con la società progettatrice della app, senza, tuttavia, far riferimento ad alcun provvedimento normativo o ad altro fondamento di liceità che legittimasse la previsione di tale strumento.

La scelta della task force del Governo è, infatti, ricaduta sull'app ideata dalla società Bending Spoons S.p.a., funzionante attraverso il Bluetooth e capace di rilevare la vicinanza di un altro smartphone entro il raggio di un metro senza ricorrere alla più invasiva "geolocalizzazione".

Le perplessità e le critiche circa la tutela dei dati personali nonché l'efficacia di tale strumento, sono state inoltre alimentate in gran parte dalla poca trasparenza e dalla scarsa diffusione di informazioni certe che non hanno fatto altro che generare apprensione nei confronti di uno strumento che sarebbe dovuto intervenire, invece, a sostegno della tutela delle persone.

Finalmente, lo scorso primo maggio è stato pubblicato nella Gazzetta Ufficiale il Decreto Legge 28/2020 recante "*Misure urgenti per la funzionalità dei sistemi di intercettazioni di conversazioni e comunicazioni, ulteriori misure urgenti in materia di ordinamento penitenziario, nonché disposizioni integrative e di coordinamento in materia di giustizia civile, amministrativa e contabile e misure urgenti per l'introduzione del sistema di allerta Covid-19*".

Si tratta di un provvedimento che seppur lacunoso risolve sicuramente la questione più importante che è, per l'appunto, quella sopra richiamata relativa all'individuazione del fondamento di liceità del trattamento, come richiesto dall'art. 9, par. 2, lett. i) del Regolamento europeo 2016/679 (GDPR) e dagli artt. 2-ter e 2-sexies del Codice Privacy.

Facciamo, dunque, chiarezza alla luce dell'entrata del nuovo Decreto Legge 28/2020, il quale all'articolo 6 si occupa specificatamente di questo strumento di *contact tracing*.

Innanzitutto, occorre richiamare il Parere n. 79 del 29 aprile 2020 del Garante Privacy nel quale viene data evidenza positiva circa la scelta di una norma di rango primario quale fondamento di liceità del trattamento. Quest'ultimo risulta, pertanto, lecito in quanto consistente nello svolgimento di un compito per esigenze di sanità pubblica previsto da una norma dello Stato.

Si tratta, per di più, di una previsione di legge che non impone alcun obbligo rimettendo alla libera volontà dei cittadini la scelta se aderire o meno a tale sistema.

La volontarietà dell'adesione mette a dura prova, tuttavia, l'efficacia stessa dell'app, la quale sarebbe assicurata solo dal raggiungimento di almeno il 60% di download da parte della popolazione italiana oltre che dall'effettivo utilizzo e dal costante impiego della connessione Bluetooth. Sul punto era, pertanto, sorto il dubbio circa la previsione di condizioni/limitazioni per cercare di raggiungere la sopra citata percentuale.

Al riguardo il Decreto Legge 28/2020 interviene, escludendo definitivamente l'ipotesi di un sistema di incentivi/limitazioni. Il comma 4 dell'articolo 6 del Decreto in esame prevede, infatti, espressamente che "il mancato utilizzo dell'app non comporta conseguenze pregiudizievoli". Tale locuzione di ampio respiro è stata adottata a seguito del Parere del Garante Privacy, il quale ha evidenziato come tale accezione sia più adatta a tradurre quello che è il principio, costituzionalmente garantito, della parità di trattamento.

Procedendo ad analizzare la norma, vediamo come il primo comma dell'articolo 6 chiarisce che il Titolare del trattamento è il Ministero della salute il quale, sentito il Ministero per gli affari regionali e le autonomie, si coordina con i soggetti operanti nel Servizio di protezione civile, nominati Responsabili esterni del trattamento ai sensi dell'art. 28 GDPR. Viene, dunque, garantita la gestione a livello statale.

Il comma 2 porta in auge, invece, il cuore di tale sistema di protezione, ossia il "progetto privacy" di fondo. La disciplina prevista dal Regolamento Europeo 2016/679 (GDPR) pone, infatti, come corollari della protezione dei dati personali i principi di privacy by design e privacy by default, richiedendo dunque che vengano predisposte tutte le misure adeguate e necessarie volte a garantire effettività al sistema di sicurezza da mettere in piedi sin dalla sua fase di progettazione.

La stessa autorità europea (European Data Protection Board) aveva specificato a riguardo come non si potesse prescindere dal rispetto del principio di accountability, ossia dalla c.d. responsabilizzazione, che avrebbe comportato innanzitutto la necessità di partire dall'analisi dell'impatto di una simile app sulla protezione dei dati personali.

È lo stesso Garante Privacy a fornire riscontro circa l'esito positivo della valutazione di impatto (DPIA) ex art. 35 GDPR, evidenziando come tale progetto garantisca la trasparenza relativamente alle modalità ed alle misure adottate nel trattamento dei dati, da riscontrare specificamente: in un'idonea informativa da fornire preventivamente all'utente, nella selettività e minimizzazione dei dati, nella reciprocità di anonimato tra gli utenti (anonimizzazione/pseudonimizzazione), nella scelta del sistema Bluetooth e nella corrispettiva assenza della geolocalizzazione (si passa, infatti, dalla dizione

di “tracciamento” a quella di “gestione del sistema di allerta”), nell’assenza del rischio di reidentificazione degli interessati, nella conservazione dei dati limitata alla fine dell’emergenza, nella cancellazione automatica dei dati e nella previsione di modalità semplificate per l’esercizio dei diritti degli interessati.

Se le ultime indiscrezioni lasciavano, inoltre, trapelare la scelta di un modello totalmente “decentralizzato”, basato sulla conservazione dei dati sui soli dispositivi individuali, in modo da minimizzare maggiormente il trattamento dei dati personali, in realtà il Decreto non prevede alcun riferimento a ciò. Rimane, dunque, sospeso tale punto, sul quale lo stesso Garante invita a fare chiarezza.

In sintesi, si tratta di uno strumento previsto da una norma di legge, il cui fine è preordinato al perseguimento di un interesse pubblico con l’esclusione di forme secondarie di trattamento dei dati personali se non in forma anonima o aggregata.

Il cuore del sistema risiede, inoltre, nell’ampia tutela accordata ai diritti dei cittadini, i quali appaiono garantiti dalla scelta di lasciare volontaria, incondizionata e priva di ogni forma di disparità di trattamento l’adesione a tale sistema, nonché dalla previsione di un’apposita informativa preventiva, dalla temporaneità della conservazione dei dati e dalle modalità agevolate per l’esercizio dei propri diritti.

Sembra, pertanto, scacciato ogni timore circa un’eventuale collisione con la tutela dei dati personali. Ci si chiede, allora se, alla luce di quanto sinora esposto, si possa effettivamente parlare di “gestione del sistema di allerta”, come suggerito dal Governo, abbandonando la più – probabilmente – temuta dicitura di “tracciamento dei contatti” e, se tale cambiamento possa portare ad una maggiore fiducia da tradurre in termini di maggiore adesione al sistema.

Ciò rifletterebbe, inoltre, l’orientamento tenuto sino ad oggi dagli Organi di Stato, icasticamente sottolineato anche dal Presidente della Corte Costituzionale, secondo cui non esiste un diritto emergenziale che legittimi la compressione e la lesione dei diritti fondamentali ma occorre guardare alla Carta costituzionale come ad una “*bussola*” capace di guidarci anche nelle situazioni più critiche come quella che stiamo vivendo.

Avv. Giuseppe Cannella (Coordinatore Comitato scientifico ASSO DPO)