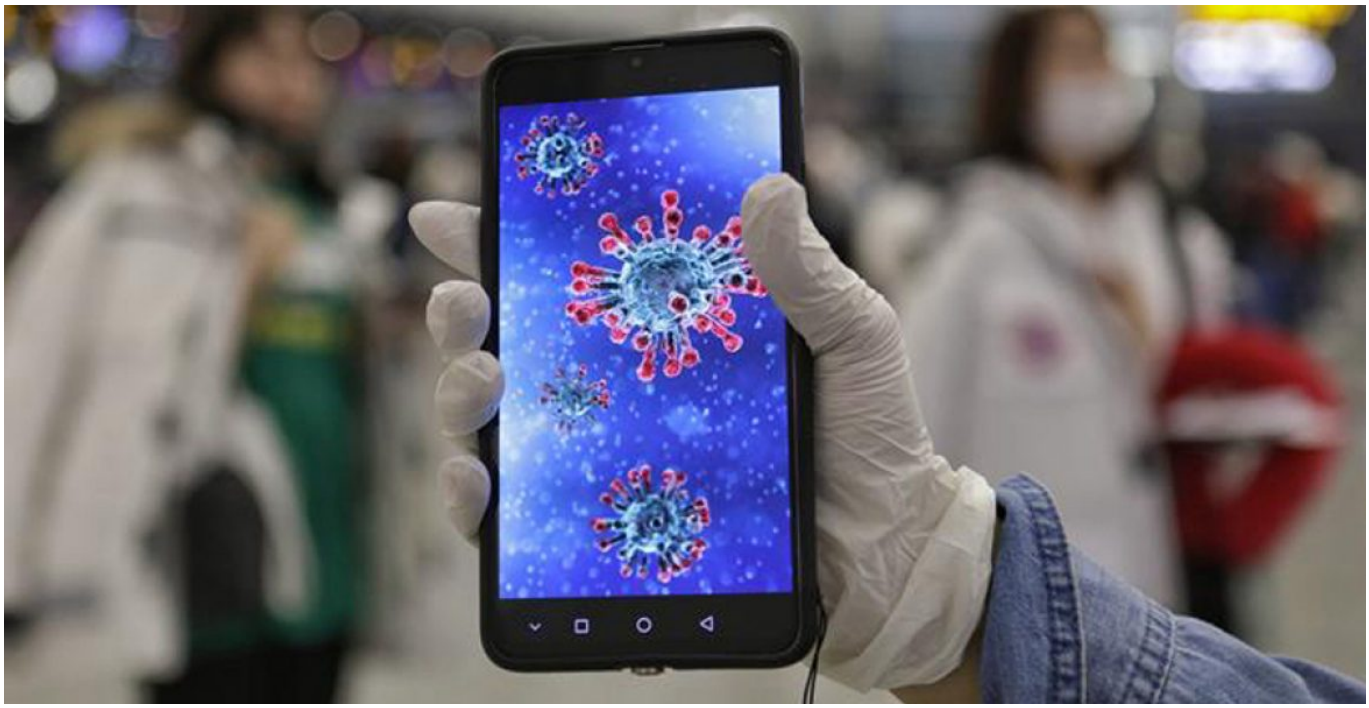
Copasir: App ‘Immuni’ è da rivedere, rischio privacy

18 Maggio 2020



L’App di contact tracing ‘**Immuni**‘ ha diversi “aspetti critici”, da correggere, “per evitare che l’efficacia della iniziativa risulti ridotta” e che vi siano “rischi connessi alla trasmissione dei dati dei cittadini nel rispetto della privacy”. E poi per la “gestione complessiva, dal punto di vista epidemiologico, dell’emergenza sanitaria”.

Così la **Relazione sul sistema di allerta CoVid19 del Copasir**, il Comitato parlamentare per la sicurezza della Repubblica segnala alcuni aspetti critici, auspicando che vengano evitati rischi per la privacy e la sicurezza. “L’alert dovrebbe essere collegato all’effettuazione di un tampone”.

La relazione, approvata dal Comitato nella seduta del 13 maggio scorso e sulla quale il M5s si era astenuto, verrà presentata al parlamento.

Il Comitato premette che “non intende entrare nel merito della scelta del governo di predisporre uno strumento di tracciamento dei contatti sociali per prevenire i rischi derivanti dal contagio Covid-19. Scelta che del resto altri Paesi hanno effettuato, o sono in procinto di effettuare, nel quadro delle iniziative volte al contenimento dell’epidemia”. Tuttavia, si legge

nella relazione, “ritiene di segnalare alcuni aspetti critici, che dovrebbero essere corretti, per evitare che l’efficacia della iniziativa risulti ridotta, e, soprattutto, che si possano determinare rischi connessi sia alla trasmissione dei dati dei cittadini, in ordine al rispetto della privacy e alla sicurezza dei dati personali, sia in particolare alla stessa gestione complessiva, dal punto di vista epidemiologico, dell’emergenza sanitaria”.

In primo luogo, segnala la relazione, “si rileva che la norma di cui al citato articolo 6 del decreto-legge n. 28 del 2020, istitutivo della piattaforma digitale, rinvia a successivi atti del ministro della Salute l’individuazione dei criteri sulla base dei quali verranno stabiliti i dati sanitari e personali da immettere nell’applicazione e le modalità con cui avverrà tale inserimento”.

Il Copasir mette in guardia anche da possibili attacchi hacker. “Non può essere sottovalutato il rischio tecnologico, anch’esso difficilmente mitigabile, almeno nel breve periodo, consistente in possibili attacchi di tipo informatico da parte di hacker o altri soggetti o in possibili truffe ai danni degli utilizzatori della app”, si legge ancora nella relazione.

“La tecnologia Bluetooth risulta infatti particolarmente vulnerabile a intrusioni i cui effetti, in questo contesto, potrebbero essere tali da diffondere allarme ingiustificato nella popolazione, ad esempio mediante l’invio di messaggi falsi o fraintendibili, relativi, inter alia, allo stato di salute o al possibile contagio dei destinatari – osserva il Copasir -. In ogni caso, il fatto che il sistema non preveda la geolocalizzazione, elemento su cui il Comitato concorda, se da un lato tutela la privacy , dall’altro esclude che si possa procedere a individuare, e quindi a sanificare, determinati ambienti o zone potenzialmente infette”.

Infine, dalle audizioni svolte non sembra praticabile una interoperabilità con le soluzioni adottate, o in via di adozione, da parte degli altri principali Paesi europei, considerato anche che non è stata decisa una linea comune a livello di Unione europea (sebbene sia stata adottata il 17 aprile scorso una comunicazione della Commissione con alcuni orientamenti per gli Stati membri circa la app di tracciamento) – conclude il Comitato -. Questo aspetto appare decisivo per la piena funzionalità del sistema, soprattutto in un Paese a vocazione turistica come il nostro, che dovrebbe assicurare la libera circolazione delle persone all’interno dell’Unione europea”.