
XVIII LEGISLATURA

Doc. XXXIV
n. 2

COMITATO PARLAMENTARE PER LA SICUREZZA DELLA REPUBBLICA

(istituito con la legge 3 agosto 2007, n. 124)

(composto dai deputati: *Raffaele Volpi*, Presidente, *Dieni*, Segretaria, *Enrico Borghi*, *Vito e Zennaro*; e dai senatori: *Urso*, Vicepresidente, *Arrigoni*, *Castiello*, *Fazzone* e *Magorno*)

RELAZIONE

sui profili di sicurezza del sistema di allerta Covid-19 previsto dall'articolo 6 del decreto-legge n. 28 del 30 aprile 2020

(Relatori: senatore Paolo ARRIGONI e deputato Antonio ZENNARO)

Approvata nella seduta del 13 maggio 2020

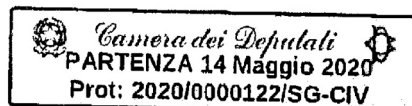
Trasmessa alle Presidenze il 14 maggio 2020



Camera dei Deputati - Senato della Repubblica

COMITATO PARLAMENTARE
PER LA SICUREZZA DELLA REPUBBLICA

IL PRESIDENTE



Signor Presidente,

nella seduta del 13 maggio 2020, il Comitato che presiedo ha approvato a maggioranza la "Relazione sui profili del sistema di allerta Covid-19, previsto dall'articolo 6 del decreto-legge n.28 del 30 aprile 2020".

Nella medesima seduta il Comitato ha, altresì, deciso - ai sensi degli articoli 35 e 37, comma 2, della legge n. 124 del 2007 - di rendere pubblica la relazione, deliberandone la presentazione al Parlamento.

Mi onoro, pertanto, di trasmettere la Relazione a Lei e al Presidente del Senato della Repubblica.

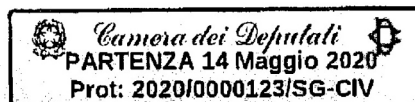
L'occasione mi è gradita per inviarLe i miei più cordiali saluti.

Raffaele Volpi

On. Roberto FICO
Presidente della Camera dei deputati

*Camera dei Deputati - Senato della Repubblica*COMITATO PARLAMENTARE
PER LA SICUREZZA DELLA REPUBBLICA

IL PRESIDENTE



Gentile Presidente,

nella seduta del 13 maggio 2020, il Comitato che presiedo ha approvato all'unanimità la "Relazione sui profili del sistema di allerta Covid-19, previsto dall'articolo 6 del decreto-legge n.28 del 30 aprile 2020".

Nella medesima seduta il Comitato ha, altresì, deciso - ai sensi degli articoli 35 e 37, comma 2, della legge n. 124 del 2007 - di rendere pubblica la relazione, deliberandone la presentazione al Parlamento.

Mi onoro, pertanto, di trasmettere la Relazione a Lei e al Presidente della Camera dei deputati.

L'occasione mi è gradita per rinnovarLe i miei più cordiali saluti.

Raffaele Volpi

Sen. Elisabetta ALBERTI CASELLATI
Presidente del Senato della Repubblica

PAGINA BIANCA

INDICE

—

	<i>Pag.</i>
Introduzione	7
Valutazioni di carattere tecnico	8
Valutazioni di carattere procedurale	9
Composizione della società proprietaria della App Immuni	11
Conclusioni	11

PAGINA BIANCA

Introduzione.

Nel corso dell'attuale legislatura, il Comitato parlamentare per la sicurezza della Repubblica, attraverso la costante interlocuzione con il DIS e con le Agenzie, ha posto al centro della propria iniziativa, tra gli altri, il tema della sicurezza cibernetica, che è stato in particolare affrontato sotto il profilo dei rischi connessi alle reti 5G (su cui è stata approvata una relazione, trasmessa al Parlamento il 12 dicembre 2019).

Tale filone di attività ha del resto assunto una rilevanza strategica nell'attuale contesto interno e internazionale, caratterizzato da una sempre maggiore pervasività delle nuove tecnologie, che impongono agli apparati di sicurezza lo sviluppo di elevate professionalità per garantire la prevenzione e il contrasto alle minacce provenienti da diversi attori (statuali, privati, *hacker*).

In tale quadro, i recenti interventi legislativi hanno notevolmente rafforzato le competenze del DIS, individuato quale centro di coordinamento della architettura nazionale di sicurezza cibernetica, mentre si sono parallelamente rafforzate le strutture dell'intero Comparto Intelligence, anche sotto il profilo delle risorse umane e finanziarie.

Presso il DIS è stato tra l'altro recentemente istituito – con DPCM 8 agosto 2019 – il CSIRT (*Computer security incident response team*), organismo destinato ad assorbire le competenze del CERT P.A. e del CERT Nazionale nelle funzioni di risposta tempestiva alle minacce cibernetiche nei confronti di soggetti pubblici e privati.

Proprio in relazione a tali funzioni, e all'esperienza maturata nell'analisi delle questioni di sicurezza connesse all'utilizzo delle tecnologie più avanzate, il DIS ha coadiuvato il Ministro della salute e il Ministro per l'innovazione tecnologica nell'istruttoria per la realizzazione della piattaforma digitale che, secondo quanto prevede l'articolo 6 del decreto-legge n. 28 del 30 aprile 2020, dovrà gestire un sistema di allerta digitale per i soggetti che abbiano installato volontariamente un'apposita applicazione (di seguito anche App), al fine di segnalare i contatti con persone risultate positive al Covid-19.

Il Comitato ha ritenuto di procedere a un approfondimento delle questioni di sicurezza nazionale connesse all'introduzione di tale applicazione digitale destinata al tracciamento dei cittadini.

Ha quindi programmato una serie di audizioni, svolte in tempi molto ristretti, che hanno permesso di acquisire informazioni specifiche sul tema, al termine delle quali il Comitato ha deliberato di riferire al Parlamento, ai sensi dell'articolo 35, comma 2, della legge n. 124 del 2007, e dell'articolo 10 del Regolamento interno.

Il Comitato ha ascoltato:

il Ministro della salute, martedì 28 aprile 2020;

il Direttore generale del DIS, martedì 28 aprile e giovedì 7 maggio 2020;

il Vice direttore generale del DIS con delega al settore *cyber*, martedì 28 aprile e giovedì 7 maggio 2020;

il Ministro per l'innovazione tecnologica e la digitalizzazione, martedì 5 maggio 2020;

il Commissario straordinario per l'attuazione e il coordinamento delle misure occorrenti per il contenimento e contrasto dell'emergenza epidemiologica Covid-19, giovedì 7 maggio 2020.

Valutazioni di carattere tecnico.

Come sostenuto dal Ministro della salute, la App di *contact tracing* (di seguito anche C.T.) è parte della strategia di contenimento dei contagi decisa dal Governo, articolata in cinque azioni che sinteticamente si possono così riassumere: 1) misure di distanziamento sociale con obbligo di mascherine e altri dispositivi di protezione individuale; 2) realizzazione di Covid hospital (strutture dedicate e non miste); 3) potenziamento delle reti territoriali per l'assistenza domiciliare; 4) effettuazione di tamponi e test sierologici; 5) utilizzo di una App per il C.T.

Per *contact tracing* si intende l'attività di tracciamento dei soggetti che potrebbero avere avuto contatti stretti con persone positive al Covid-19, come previsto dall'articolo 6 del decreto-legge n. 28 del 30 aprile 2020. Tale modalità, nelle intenzioni della norma, dovrebbe essere complementare alle ordinarie modalità in uso nell'ambito del Sistema sanitario nazionale.

L'attività di *contact tracing*, secondo quanto riferito nel corso delle audizioni svolte, può essere realizzata con applicazioni informatiche tramite tecnologia Bluetooth, GPS o celle telefoniche.

La soluzione individuata dal governo è quella di un sistema di C.T. basato su tecnologia Bluetooth-LE (*low energy*), con modalità decentralizzata.

Tale scelta permette di verificare i contatti della persona, senza bisogno di geolocalizzazione; consente quindi di capire chi è stato vicino, per quanto tempo e a quale distanza, ma senza tracciare i movimenti. Per il funzionamento della App occorre che il Bluetooth sia attivato.

Si tratta però di stabilire criteri precisi, ancora non individuati nel citato decreto-legge, per definire quali possano essere considerati « contatti qualificati », cioè quelli che facciano scattare un *alert*, che segnali agli utenti di essere entrati in contatto stretto con un utente risultato positivo al virus, e dunque di essere a potenziale rischio di infezione.

Come si specificherà nelle conclusioni, tale *alert* dovrebbe essere collegato all'effettuazione di un tampone, che al momento appare l'unica modalità certa per verificare il contagio al Covid-19 di un soggetto.

Dovrebbero essere inoltre chiariti sia il meccanismo sia la responsabilità della immissione dei dati nella App. Tali dati, secondo il citato articolo 6, dovranno essere resi anonimi o, se ciò non sia possibile, pseudonimizzati.

L'architettura del sistema con modalità decentralizzata è caratterizzata dall'assenza di un *database* centrale e dalla presenza, elaborazione e conservazione dei dati unicamente sui cellulari degli utilizzatori. Tale scelta è stata orientata dalla soluzione offerta da

Apple e Google, che sembra meglio rispondere alle esigenze di fruibilità della App, considerata la penetrazione sul mercato dei due sistemi operativi (rispettivamente iOS e Android) prodotti da queste due società americane. Peraltro, anche in considerazione di questa importantissima necessità, essa presenterebbe un maggior livello di *privacy*, giacché le informazioni relative ai contatti resterebbero sul dispositivo mobile dell'utente fino al momento in cui questi non risultasse positivo al Covid-19.

Quanto agli altri Paesi, le uniche informazioni acquisite nel corso delle audizioni riguardano la Germania, che sarebbe orientata verso un sistema decentralizzato, attraverso consorzi nazionali, e la Francia, che opterebbe, con tutte le difficoltà del caso, per un sistema centralizzato, con un centro dati (*cloud*) nazionale.

In Italia non si è scelta la soluzione centralizzata perché, secondo quanto riferito nel corso delle audizioni svolte, parrebbe non essere disponibile la tecnologia necessaria ad attuare una piattaforma digitale idonea *in house*.

Di fatto, quindi, la soluzione decentralizzata risulterebbe essere stata suggerita — secondo quanto riferito nel corso delle audizioni — oltre che da considerazioni legate alla *privacy* dei dati, dal fatto che per garantire il funzionamento corretto dell'App stessa è indispensabile utilizzare le nuove API (*Application Programming Interface*) di sistema operativo dei dispositivi mobili rese disponibili da Apple e Google, che sono state progettate per questo tipo di architettura.

L'architettura decentralizzata richiede necessariamente l'utilizzo di un Content Delivery Network (CDN), unico strumento che consenta di gestire efficacemente la mole di connessioni che si prevede per il funzionamento della App.

Questa tecnologia può essere oggi erogata sul territorio nazionale, tuttavia, non essendo al momento disponibile presso aziende italiane, dovrà essere acquisita ricorrendo a società estere, ancora da individuare.

I dati sarebbero messi a disposizione del Servizio sanitario nazionale e gestiti, anche in forma aggregata o comunque anonima, dal Ministero della salute, responsabile in ultima analisi del trattamento degli stessi, tramite la società Sogei. Compito della Sogei — con cui è ancora in corso la stipula di una convenzione — dovrebbe essere la gestione delle infrastrutture del sistema, la gestione del servizio di CDN e la garanzia della sicurezza cibernetica.

Rimane tuttavia da chiarire quali misure siano previste in caso di immissione di dati inesatti, sia per errori umani sia a seguito di attacchi informatici, oppure di vere e proprie emergenze, quali ad esempio la perdita dei dati (*Disaster recovery*).

Valutazioni di carattere procedurale.

La scelta della applicazione è avvenuta, a seguito di una procedura molto rapida, consistente in una *fast call*, indetta dal Ministro per l'innovazione tecnologica, conclusasi nell'arco di tre giorni (24-26

marzo), tramite l'individuazione della App di proprietà della società Bending Spoons S.p.A.

Al fine di esaminare e selezionare le candidature è stato costituito un gruppo di lavoro (*data driven*), articolato in 8 sottogruppi, che, dopo avere verificato i requisiti delle 319 società che hanno partecipato alla *call*, ha individuato due App ritenute teoricamente valide per essere testate in parallelo a scopo di implementazione: Immuni e CovidApp.

La scelta di sviluppare il progetto esecutivo per una sola App (e il fatto che tale scelta sia ricaduta su Immuni) è stata adottata dal Ministro per l'innovazione tecnologica e dal Ministro della salute, avendo anche ascoltato il parere tecnico del DIS, in rappresentanza del Comparto, che ha considerato, viste le strette tempistiche imposte, troppo dispersivo procedere con un test parallelo su entrambe le applicazioni.

La decisione di sviluppare la App Immuni è stata assunta, secondo quanto riferito dal Ministro per l'innovazione tecnologica, in considerazione del maggiore stato di avanzamento e della possibilità di renderla quindi operativa in tempi più rapidi. Si è trattato quindi di una scelta adottata a prescindere da ogni valutazione sulla composizione societaria dei gruppi proprietari delle due App, considerata invece meritevole di approfondimento da parte del Comitato (vedi *infra*).

Inoltre, la soluzione Immuni utilizza la tecnologia della tracciabilità sviluppata dal Consorzio Progetto Europeo PEPP-PT, che in assenza di geolocalizzazione memorizzerebbe il codice identificativo anonimo dei cellulari di tutte le persone con cui si interagisce e che risulterebbe poter fornire maggiori garanzie di anonimizzazione dei dati personali.

Nella fase successiva a tale decisione, il DIS, su mandato del Presidente del Consiglio, ha proceduto a definire una griglia tecnica con i criteri ritenuti più idonei per garantire la tutela della sicurezza, sotto il profilo della crittografia e della *privacy* dei dati. In particolare, è stata sottolineata l'importanza di valutare il sistema nella sua complessità di sviluppo, non limitandosi al solo aspetto tecnico legato all'App. Ad esempio, è stata segnalata l'esigenza che l'intero sistema di C.T. sia gestito da uno o più soggetti pubblici e che il suo codice sia aperto (*open source*), che la gestione e la conservazione dei dati avvenga sul territorio nazionale, e che venga individuato un responsabile del progetto con ampia esperienza nel settore dei sistemi informatici complessi, non essendo ad oggi disponibili *best practices* che garantiscano in assoluto il buon esito del progetto, che dovrebbe assicurare sia l'aspetto della funzionalità, sia quello della sicurezza e della *privacy* nel trattamento dei dati.

All'esito della procedura sopra descritta (*fast call*, individuazione di due App, decisione di procedere con la sola App Immuni a seguito del parere del DIS, lettera del Ministro per l'innovazione tecnologica, confermata dal Ministro della salute), il Commissario straordinario per l'emergenza Covid-19 è stato incaricato dal Presidente del Consiglio di sottoscrivere il contratto con Bending Spoons S.p.A.

Il contratto prevede, in particolare, la cessione della licenza d'uso aperta, gratuita, perpetua e irrevocabile del codice sorgente della App Immuni e di tutte le componenti applicative facenti parte del sistema di C.T. già sviluppato, nonché, per le medesime ragioni e sempre a titolo gratuito, la disponibilità a completare gli sviluppi informatici che si dovessero rendere necessari per consentire la messa in esercizio del sistema nazionale di C.T. digitale.

Per quanto riguarda le successive revisioni e manutenzioni della applicazione che dovessero rendersi necessarie, il Commissario ha sottoscritto una convenzione a titolo gratuito con la società PagoPA S.p.A., interamente partecipata dallo Stato e vigilata dalla Presidenza del Consiglio.

Tuttavia, si evidenzia che all'articolo 3 del contratto già sottoscritto con Bending Spoons, la società si impegna a « *provvedere all'ulteriore sviluppo, a "regola d'arte" e con diligenza professionale, dell'App e di tutte le sue componenti e all'attività di test, collaudo, assistenza e manutenzione correttiva [...] Le predette attività cesseranno in ogni caso salvo espressa e consensuale proroga, decorsi sei mesi dalla sottoscrizione del contratto stesso* ».

Allo stato attuale non è dato sapere quali siano le caratteristiche tecniche minime dei cellulari per consentire l'installazione e il funzionamento della App.

Composizione della società proprietaria della App Immuni.

La società Bending Spoons S.p.A. è stata fondata nel 2013 da quattro cittadini italiani (Luca Ferrari, Francesco Patarnella, Matteo Danieli, Luca Querella) e da Tomasz Greber, di origine polacca. L'analisi della compagine sociale ha consentito di rilevare che i quattro fondatori italiani detengono circa l'80 per cento dell'azienda, mentre il socio Greber possiede una partecipazione del 4 per cento.

Dal 4 luglio del 2019 è presente una quota di minoranza, pari al 5,7 per cento, di proprietà dei gruppi: H14 S.p.A., NUO Capital, riconducibile alla famiglia Pao Cheng di Hong Kong, e Star Tip S.p.A., veicolo della società di investimento internazionale Tamburi Investment. Il fondo NUO Capital (*New Understanding Opportunities*), sopra citato, riconducibile a Stephen Cheng, noto uomo d'affari cinese, è stato fondato nel 2016.

In proposito, si ricorda che la legge cinese sulla sicurezza nazionale, obbliga, in via generale, cittadini e organizzazioni a fornire supporto e assistenza alle autorità militari di pubblica sicurezza e alle agenzie di intelligence.

La composizione societaria del restante 10,3 per cento risulta suddivisa in piccole quote azionarie di proprietà di ex dipendenti della società stessa.

Conclusioni.

Il Comitato 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.

Il Comitato ritiene, però, 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, 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. Pertanto, il citato articolo 6 costituisce soltanto una cornice del progetto, i cui dettagli, molti dei quali rilevanti, devono essere ancora individuati e determinati, attraverso atti di natura amministrativa.

Ad esempio, il sistema di C.T. viene definito complementare rispetto alla ordinaria modalità in uso nell'ambito del SSN, mentre il Comitato ritiene che esso dovrebbe essere considerato integrativo di tali modalità, per evitare che il C.T. digitale sostituisca il tracciamento ordinario.

La norma inoltre prevede che il tracciamento riguarderà solo le persone risultate positive al Covid-19, ma, a tale riguardo, il Comitato ritiene che l'unico dato da dover immettere nella App dovrebbe essere un codice anonimo risultante dall'effettuazione di un tampone, escludendo quindi altre procedure che al momento non abbiano evidenza scientifica.

La norma peraltro sul punto non chiarisce qual è il soggetto titolato ad inserire nella App tale codice anonimo, e inoltre non definisce controlli e disposizioni in ordine a quale sia la conseguenza di un *alert*, cioè quali comportamenti dovranno essere adottati da chi riceve la notifica di avere avuto contatti con una persona risultata positiva al Covid-19 e quali eventuali conseguenze derivino dalla mancata adozione degli stessi.

In generale, appare necessario che l'attuazione della piattaforma avvenga con criteri univoci sul territorio nazionale, evitando la possibilità di interpretazioni restrittive o comunque differenziate da parte delle Regioni ed Enti locali, tali da introdurre ingiustificate limitazioni alla libera circolazione dei cittadini. In proposito, il comma 4 del citato articolo 6 del decreto-legge n. 28 dispone che « *Il mancato utilizzo dell'applicazione [...] non comporta alcuna conseguenza pregiudizievole ed è assicurato il rispetto del principio di parità di trattamento* ».

Il Comitato ritiene che tale disposizione possa risultare insufficiente a escludere eventuali provvedimenti più restrittivi, da parte di soggetti istituzionali o da privati, volti a selezionare l'accesso delle persone (a luoghi, zone territoriali, locali pubblici o privati eccetera),

sulla base dell'utilizzo o del mancato utilizzo dell'applicazione. Tale eventualità sarebbe infatti in netta contraddizione con quanto dispone il comma 1 dell'articolo 6 circa l'installazione su base volontaria dell'applicazione di *contact tracing*.

Più in generale, si tratta, a parere del Comitato, di evitare che si determinino facilitazioni o discriminazioni connesse all'utilizzo, o mancato utilizzo, della App.

Tale preoccupazione è legata anche alla necessità, pubblicamente espressa, che l'utilità della App possa essere assicurata da un numero consistente di adesioni (quale che esso sia). Non è emerso dalle audizioni svolte quale base numerica di volontari sia adeguata alla finalità per cui è stata pensata la piattaforma; è inoltre evidente che se al numero di adesioni non corrispondesse la capacità organizzativa di effettuare tamponi, l'efficacia della misura sarebbe molto limitata, a fronte di una rilevante cessione di dati personali.

Si evidenzia inoltre la necessità di rispettare rigorosamente il termine massimo del 31 dicembre 2020, previsto dall'articolo 6, comma 6, del citato decreto, entro il quale dovrà cessare l'utilizzo della piattaforma e i dati dovranno essere cancellati o resi definitivamente anonimi.

Sulla base di quanto sopra esposto, si possono inoltre evidenziare rischi non trascurabili sul piano geopolitico, che secondo quanto emerso dalle audizioni sarebbero non mitigabili. Infatti, la definizione dettata da privati dell'architettura dell'intero sistema informatico, inclusa la App, nonché la necessità di ricorrere a soggetti privati non nazionali, per quanto da considerare affidabili, per il CDN destinato a contenere i dati raccolti, potrebbero prestarsi a manipolazioni dei dati stessi, per finalità di diversa natura: politica, militare, sanitaria o commerciale. Si sottolinea inoltre come la possibile alterazione dei dati potrebbe far sovrastimare o sottostimare l'entità stessa dell'epidemia.

Va inoltre evidenziato come, qualora ciò dovesse essere confermato, la soluzione di trasmettere i dati dei cittadini italiani alla Content Delivery Network pare contrastare con il contenuto dell'articolo 6, comma 5, del decreto-legge n. 28 del 30 aprile 2020, in cui si esplicita in maniera chiara che la piattaforma, di titolarità pubblica, è realizzata esclusivamente con infrastrutture localizzate sul territorio nazionale e gestite dalla società di cui all'articolo 83, comma 15, del decreto-legge 25 giugno 2008, n. 112, convertito, con modificazioni, dalla legge 6 agosto 2008, n. 133. Peraltro, appare quanto mai opportuno porre all'attenzione anche che, alla luce del comma 3 dell'articolo del citato decreto-legge, i dati raccolti attraverso l'applicazione non potranno essere trattati per finalità diverse da quella di allertare le persone che siano entrate in contatto stretto con soggetti risultati positivi e tutelarne la salute, salva la possibilità di utilizzo in forma aggregata o comunque anonima, per soli fini di sanità pubblica, profilassi, statistici o di ricerca scientifica. Per quanto appena evidenziato, un simile « transito di dati » — anche se fosse temporaneo e avvenisse esclusivamente per mezzo di sistemi informatici presenti sul territorio nazionale — dovrebbe obbligatoriamente essere non solo chiarito ed esplicitato, ma anche e soprattutto regolamentato con estrema attenzione sotto il punto di vista giuridico, al fine di

adempiere a quanto previsto dalla normativa europea e nazionale in materia di trattamento di dati personali.

In tal senso, potrebbe essere opportuno verificare che nessun attore nazionale e soprattutto internazionale, ivi compresa la società aggiudicataria dello sviluppo della App, possa in qualsivoglia modo accedere direttamente o incidentalmente ai dati raccolti, anche nel caso in cui questo soggetto abbia dato un qualsiasi apporto — anche tecnologico — per la realizzazione o per l'efficacia del sistema nazionale di allerta Covid-19. Ciò al fine di impedire che simili informazioni — rilevanti sia sul piano della qualità sia della quantità e soprattutto della capillarità — possano più o meno direttamente entrare nel possesso di attori europei e internazionali, sia pubblici sia privati, a vario titolo interessati.

Il Comitato esprime preoccupazione per il fatto che dopo l'entrata in esercizio della App Immuni, che dovrà comunque essere preceduta da fasi di test, la Bending Spoons, secondo quanto previsto dal contratto, continuerà la sua attività di aggiornamento dell'applicazione per un periodo di sei mesi, determinando quindi una potenziale dipendenza del sistema posto in essere da tale sviluppo tecnologico, affidato anche in questo caso a una società privata. Sul punto non risulta chiaro se l'attività di aggiornamento della App da parte di Bending Spoons possa svolgersi in sovrapposizione e/o congiuntamente con l'attività di PagoPA.

Né 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. 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.

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). 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.

PAGINA BIANCA



180340101730