MINISTRO
PER L'INNOVAZIONE
TECNOLOGICA
E LA DIGITALIZZAZIONE

CONFIDENZIALE

Report sottogruppo di lavoro 6

Report sulle attività svolte dal sottogruppo di lavoro impegnato nell'individuazione di "Tecnologie per il governo dell'emergenza" (in particolare contact-tracing) mediante valutazione di 319 soluzioni tecnologiche pervenute con call for contribution dal 24 al 26 Marzo.

Coordinatori:
Fidelia Cascini, Università Cattolica S. Cuore
Paolo De Rosa, Dipartimento per la trasformazione digitale

Componenti del sottogruppo:
Francesca Bria, UCL London e Fondo Innovazione
Carlo Alberto Carnevale Maffè, Università Bocconi, Milano
Ciro Cattuto, Università di Torino
Leonardo Favario, Dipartimento per la trasformazione digitale
Alfonso Fuggetta, Politecnico di Milano
Andrea Nicolini, Fondazione Bruno Kessler
Alberto E. Tozzi, Ospedale Pediatrico "Bambino Gesù", Roma
Simone Piunno, Università Bocconi, Milano
Stefano Calabrese, Dipartimento della Protezione Civile
Umberto Rosini, Dipartimento della Protezione Civile

Premessa

Le esperienze internazionali maturate in questi ultimi mesi, a partire dall'insorgenza dell'epidemia COVID-19, dimostrano che alcune soluzioni tecnologiche sono state in grado di ricostruire tempestivamente una precisa mappa dei contatti tra individui con infezione e individui sani offrendo un importante strumento operativo per azioni di prevenzione. Il tracciamento dei contatti *(contact tracing*) con adeguate tecnologie consente di ricostruire catene di potenziale contagio nel rispetto delle normative vigenti in materia di protezione dei dati personali. L'uso di queste tecnologie si è già dimostrato efficace nella strategia di contenimento dell'infezione da SARS-COV-2 in altri Paesi. In Corea del Sud, ad esempio, è stata osservata [1] - grazie all'utilizzo di Big Data nella mappatura e nel contenimento dell'epidemia - una diminuzione nel tempo del tasso effettivo di riproduzione del contagio (R_0), ottenuto individuando tempestivamente e precisamente gli *hot spot* di potenziale contagio concentrando su di esse le azioni di prevenzione. La sfida sarà quindi quella di isolare i casi confermati e i loro contatti rispettando i diritti e le libertà fondamentali proprie delle democrazie europee.
Nonostante le molte obiezioni inizialmente sollevate contro l'efficacia del *contact tracing*, le più recenti ricerche scientifiche sull'epidemia COVID-19 [2] dimostrano che la sola esecuzione di test diagnostici non è sufficiente per ridurre la trasmissione dei contagi perché il tempo necessario per il riconoscimento dei casi ritarda le altre azioni di prevenzione. Di fatto, le manifestazioni cliniche di COVID-19 possono essere assenti o impiegare alcuni giorni per esprimersi, ritardando il riconoscimento dei casi con infezione. A questo si aggiunge il tempo necessario per ricevere i risultati dei test diagnostici. Tale latenza si riflette sulla tempestività delle misure di isolamento dei soggetti infetti. La ricerca scientifica evidenzia in particolare che la malattia risulta asintomatica fino al 55% delle trasmissioni con un *generation period* molto breve (3-5 giorni). La ricostruzione della catena trasmissiva del virus a partire dal solo esito dei test diagnostici è pertanto insufficiente e tardiva (prova ne è il fatto che l'isolamento dei positivi non ha effetti risolutivi sulla riduzione di R_0 al di sotto dell'unità).

Il lavoro di Ferretti et al. [2], dimostra come anche ad elevatissimi livelli di successo nell'isolamento dei casi positivi, serva una rapida e ampia identificazione e messa in quarantena almeno dei contatti di primo livello per poter mettere sotto controllo l'epidemia. Attualmente, ricostruire "manualmente" i contatti di un malato di COVID-19 si sta rivelando un'attività lenta e farraginosa. Il Big Data Institute di Oxford propone[1] quindi un *workflow* di riferimento per lo sviluppo di soluzioni tecnologiche specificamente destinate al *contact tracing* per COVID-19, che recepisca i principali elementi etici e scientifici emersi dalle

[1] https://bdi-pathogens.shinyapps.io/covid-19-transmission-routes/

ultimissime ricerche in merito. Il modello del Big Data Institute si basa sulle migliori pratiche studiate nei modelli internazionali di contrasto all'epidemia COVID-19 e delinea lo schema di tracciabilità istantanea dei contatti di primo grado: un sistema di *alerting* su smartphone è in grado di informare gli utenti, in base alla loro matrice di contatti ed eventualmente alla loro posizione geografica, rispetto a quando possono spostarsi in sicurezza, quando devono cercare assistenza medica, quando devono evitare persone vulnerabili. Il modello proposto ha il potenziale di rallentare drasticamente la diffusione dell'epidemia se utilizzato da un numero sufficientemente ampio di persone che ne facciano uso con adeguata fedeltà.

In linea con le suddette pubblicazioni, le indicazioni fornite dall'OMS al momento della dichiarazione della pandemia sono apparse chiare ed esplicite indicando testualmente: "*Find, isolate, test and treat every case and trace every contact*". Perciò, mettere a punto processi e tecnologie allo scopo di tracciare rapidamente i contagi, è essenziale per circoscrivere e contrastare l'espandersi delle catene di trasmissione del virus, anche nei Paesi che, come l'Italia, applicano drastiche forme di contenimento generalizzato (*lockdown*).

Allineata su questi stessi obiettivi, l'attività svolta dal sottogruppo di lavoro impegnato sulla disamina di tecnologie 'data driven' per la gestione dell'emergenza in atto, è dedicata a supportare le decisioni delle autorità politiche affinché possano essere facilitate nel perseguire il triplice obiettivo di: a) provvedere alla tutela della salute pubblica, b) ripristinare il più rapidamente possibile le condizioni permissive delle attività economiche e commerciali dopo il *lockdown*, c) consentire il recupero della mobilità personale sotto monitoraggio permanente di eventuali focolai di ripresa garantendo al contempo il diritto alla riservatezza e alla protezione dei dati personali.

Verso un modello europeo

La pandemia COVID-19 rappresenta una grave minaccia per i paesi di tutto il mondo e in particolare per i paesi dell'Unione Europea, al momento tra i più colpiti. Nell'UE, infatti, il virus si è diffuso rapidamente e non conosce confini geografici o politici. Per metterlo sotto controllo, si deve agire allo stesso modo: la velocità e la cooperazione internazionale risultano quindi essenziali per contrastarne l'avanzata. In risposta al numero in rapida crescita di casi e al pericolo di sovraccaricare i sistemi sanitari, molti paesi hanno imposto vincoli agli spostamenti o adottato blocchi delle attività economiche e sociali per rallentare la diffusione

del coronavirus. Poiché un blocco a lungo termine non è economicamente e socialmente sostenibile, alcuni soggetti pubblici e privati europei si sono attivati per elaborare una risposta comune che, attraverso soluzioni tecnologiche interoperabili di *contact tracing*, consenta di mantenere una società e un'economia aperte, proteggendo la salute dei cittadini senza rischiare il collasso del sistema sanitario.

La selezione della soluzione tecnologica di riferimento a livello europeo è stata proposta dal consorzio internazionale Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT)[2], che conta oltre 130 membri in otto paesi europei e include eccellenze europee nel campo della ricerca scientifica e tecnologica, tra cui anche centri di ricerca italiani. PEPP-PT si basa su un approccio condiviso con le seguenti caratteristiche fondamentali:

- Procedure collaudate e consolidate per la misurazione della prossimità tra device (smartphone) su sistemi operativi e dispositivi mobili di grande diffusione.
- Protezione crittografica dei dati, anonimizzazione, conformità al GDPR ed elevata cybersecurity.
- Interoperabilità internazionale e interregionale per supportare il tracciamento delle catene locali di infezione anche se una catena si estende su più paesi o su più regioni.
- Architetture e tecnologie di back-end scalabili che possano essere implementate con l'infrastruttura IT locale.
- Un servizio di certificazione del codice open source per testare e garantire che le diverse implementazioni utilizzino i meccanismi in modo sicuro e interoperabile.
- Implementazione di riferimento disponibile sotto la licenza open source *Mozilla License Agreement.*

La tecnologia proposta dal Consorzio Europeo può dare un contributo decisivo a un tracciamento di prossimità efficiente e molto più rapido di quello tradizionale, nel rispetto dei diritti e delle libertà fondamentali dei cittadini, comprese garanzie rispetto al trattamento dei loro dati personali, in linea con i valori e le norme europee.
Per questo motivo si è attivato il processo per selezionare una soluzione tecnica che renda possibile il tracciamento della prossimità tramite *smartphone*, così che non vengano tracciate le persone fisiche e non vengano estratti i loro dati personali (es. chi siano e dove sono stati); si punta a tracciare solo le relazioni di prossimità a corto raggio che costituiscono rischio di esposizione e corrispondono a potenziali catene di trasmissione del virus. Il punto di partenza naturale per tali processi sono i telefoni cellulari poiché la maggior parte delle persone usa regolarmente questo tipo di device e anche coloro che dovessero ancora esserne privi possono essere equipaggiati in modo rapido ed economico.

[2] Pan-European Privacy-Preserving Proximity Tracing, PEPP-PT, https://www.pepp-pt.org

Lo sviluppo di questa tecnologia si basa su tre principi di base. Innanzi tutto, è il risultato di una analisi dei *benchmark* internazionali e di un forte spirito di cooperazione europea. In secondo luogo, la tecnologia viene studiata e selezionata per essere applicabile a livello internazionale, vale a dire interoperabile oltre i confini nazionali. In tal modo, la tecnologia faciliterà la ripresa di regolari relazioni internazionali e la libertà di circolazione dei cittadini. In terzo luogo, la tecnologia individuata deve essere conforme con il regolamento generale sulla protezione dei dati (GDPR).

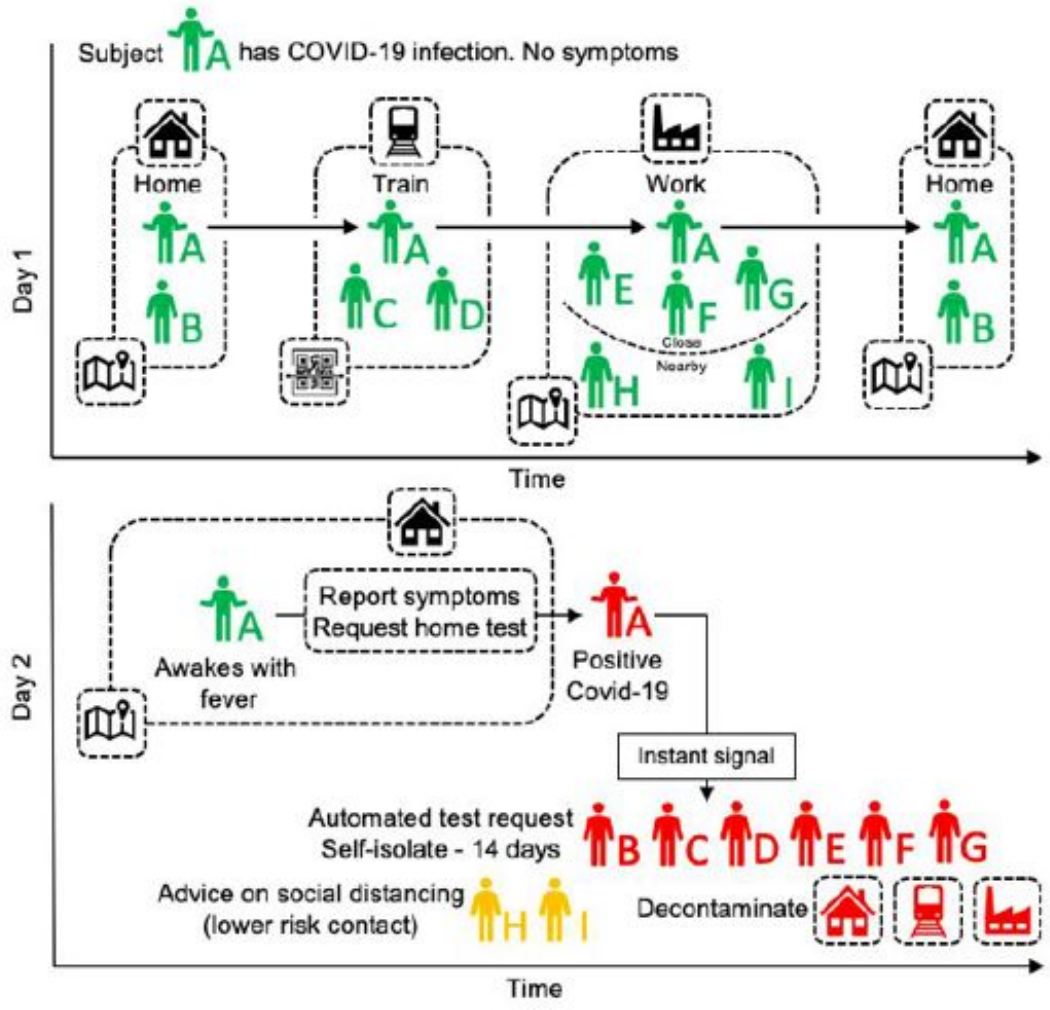
Lo sviluppo di un tale sistema è una grande sfida, ma che vale la pena raccogliere. Come è successo anni fa con la creazione dei primi standard europei per la telefonia cellulare GSM, cresciuta nell'adozione internazionale fino a diventare uno standard globale, la tecnologia di base deve fornire un meccanismo di tracciamento della prossimità applicabile in modo omogeneo anche al di fuori dei singoli confini nazionali. Sulla base di esso, ogni paese potrà sviluppare la propria versione locale di app e fornire la propria infrastruttura sicura. Ciò consentirà a ciascun paese partecipante di applicare operativamente la soluzione tecnologica in coordinamento con le autorità sanitarie locali per le esigenze della popolazione locale. Ogni paese deve anche essere in grado di informare in modo trasparente i propri cittadini così da convincerli, senza usare imposizioni autoritarie, a partecipare volontariamente a tale sistema. La tecnologia di base, sviluppata in costante confronto con autorevoli esperti di diverse discipline, dovrà fornire un contributo importante per consentire il tracciamento della prossimità, anche in modalità transfrontaliera, nel rispetto della privacy, secondo un modello scalabile e aperto, che possa essere utilizzato da qualsiasi paese.

La selezione delle soluzioni è stata quindi orientata al pieno rispetto delle leggi e dei principi europei in materia di privacy e protezione dei dati. I meccanismi e gli standard tecnici ricercati sono quindi orientati a tutelare la privacy, la trasparenza e la sicurezza nella gestione dei dati, sfruttando le possibilità della tecnologia digitale per massimizzare la velocità e la capacità in tempo reale di risposta alla pandemia. Questi meccanismi includono tecnologie di tracciamento della prossimità collaudate, anonimizzazione dei dati sicura e crittografata, meccanismi affidabili per consentire il contatto tra l'utente e i funzionari sanitari in un ambiente conforme alla protezione dei dati, interfacce di scambio di dati digitali (API) in grado di fornire catene di contatti anonimizzate e valutazione del rischio ad altre applicazioni (ad esempio per la gestione delle risorse sanitarie, la gestione del rischio privato o i sistemi di risposta alla pandemia).

L'implementazione di riferimento deve basarsi su codice open source, con servizi di backend sicuri e scalabili in grado di gestire centinaia di milioni di dispositivi registrati, servizi di supporto per l'interoperabilità transfrontaliera, la divulgazione e l'adozione da parte di una massa critica di cittadini.

Digital contact tracing

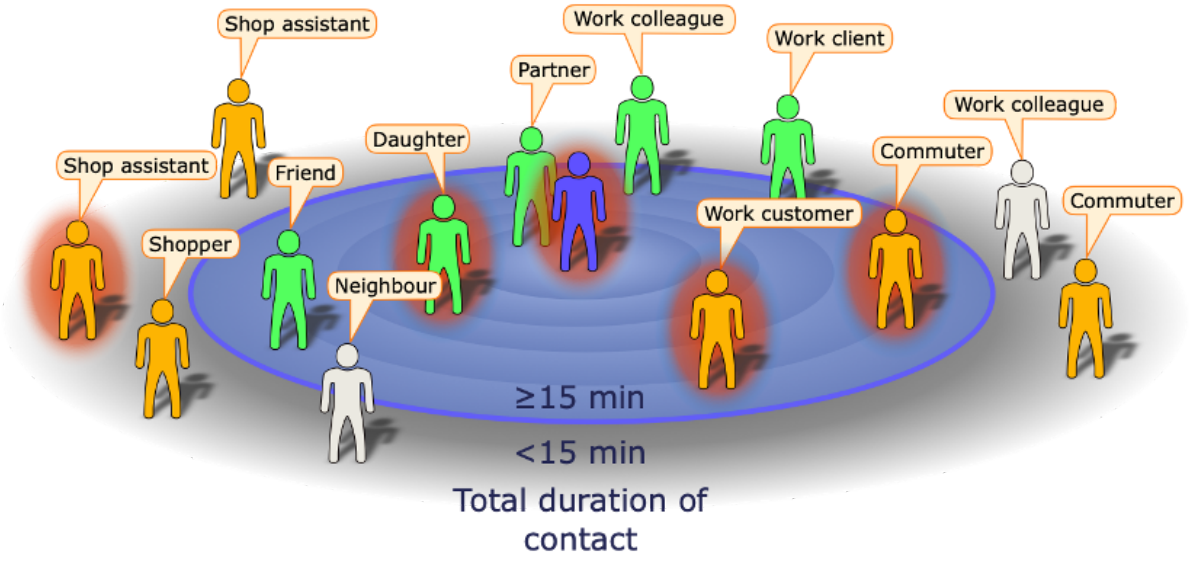
A titolo illustrativo, si descrive qui di seguito il funzionamento generale di una soluzione per il *contact tracing* digitale, in grado di valutare il rischio di trasmissione del virus attraverso monitoraggio del numero, della durata e del tipo di contatti, attraverso un normale *smartphone*. Lo schema sottostante propone un processo operativo di riferimento per le soluzioni tecnologiche destinate al *contact tracing* per COVID-19. Il modello, derivato dalle ricerche del Big Data Institute di Oxford University, si basa sulle migliori prassi studiate nei modelli internazionali di contrasto all'epidemia COVID-19 e delinea lo schema di tracciabilità istantanea dei contatti di primo grado basato su una app da installare sul proprio *smartphone* e da una infrastruttura di gestione (*backend*) sotto il controllo delle autorità sanitarie.



Nel pannello in alto la figura illustra i possibili contatti tra individui durante le attività quotidiane come ad esempio nei mezzi di trasporto o nell'ambiente di lavoro. Nel pannello in basso viene illustrata la serie di interventi di isolamento e distanza sociale che possono essere messi in atto immediatamente dopo che il soggetto positivo a SARS-COV2 viene segnalato come positivo ai propri contatti dei giorni precedenti attraverso l'applicazione su smartphone. Fonte: Sustainable containment of COVID-19 using smartphones in China: Scientific and ethical underpinnings for implementation of similar approaches in other settings, David Bonsall, Michael Parker, Christophe Fraser, Big Data Institute, 16 February 2020.

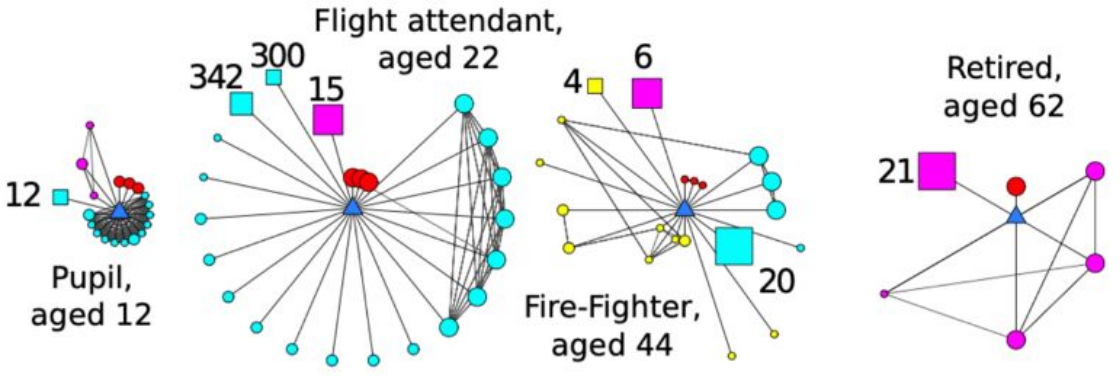
La soluzione proposta nel modello europeo, sopra indicato, non raccoglie in via ordinaria dati personali, né altri dati che consentano l'identificazione del proprietario del dispositivo mobile. La soluzione di contact tracing normalmente tiene traccia del solo numero, durata e tipo di contatti ravvicinati con altri device nei quali risulta attiva la stessa soluzione. Tuttavia sussiste il rischio che nel corso del funzionamento della soluzione vengano raccolti dati che potrebbero compromettere la natura anonima dei dati trattati in via ordinaria.
L'utente non viene necessariamente geolocalizzato (sebbene ciò possa essere tecnicamente reso possibile, purchè dietro specifica e consapevole scelta di opt-in da parte dell'utente), né viene reso riconoscibile, salvo che accetti esplicitamente tali opzioni, laddove applicabili e disponibili. In caso di contagio, le informazioni sono condivise con le sole autorità sanitarie. Utilizzando metodi di trasmissione dei dati orientati alle SAN (Small Area Network) quali ad esempio ANT, BT-LE, BT, AUDIO e WiFiP2P in funzione della sensoristica disponibile sul dispositivo e incrociando (ove possibile e sempre dietro esplicita autorizzazione dell'utente) i dati di posizione provenienti da GPS e Network Position (triangolazione basata su celle telefoniche), il telefono acquisisce un ID univoco e crittografato di tutti gli smartphone in prossimità (circa 1-2 m., ma in certi casi anche oltre) e conserva la durata e la distanza stimata di tale contatto ravvicinato. La scansione avviene a periodi programmabili di alcuni secondi, anche con l'app in *background*. Le tecnologie selezionate devono poter tracciare i contatti in prossimità del soggetto potenzialmente infetto con una precisione molto elevata, nell'ordine di poche decine di centimetri.

Con riferimento al *contact tracing* tradizionale, si veda la successiva rappresentazione grafica degli incontri fatti durante il giorno da un caso di paziente infettivo (blu) con i contatti posizionati in base alla durata totale del contatto. Nello schema sottostante, la definizione di "contatto" è relativa a qualcuno con cui il soggetto infettivo si è incontrato per 15 minuti o più. Alcuni contatti saranno tracciabili (verde), mentre altri non saranno tracciabili (arancione). Una definizione di contatto troppo restrittiva e inappropriata per l'infezione da COVID-19 implicherebbe che alcuni incontri potrebbero non riuscire a soddisfare la definizione, ma potrebbero essere comunque a rischio di infezione; a loro volta, questi contatti esclusi potrebbero essere tracciabili (grigio chiaro) o non tracciabili (arancione).



Fonte: Matt J Keeling et al., The Efficacy of Contact Tracing for the Containment of the 2019 Novel Coronavirus (COVID-19), medRxiv doi: https://doi.org/10.1101/2020.02.14.20023036

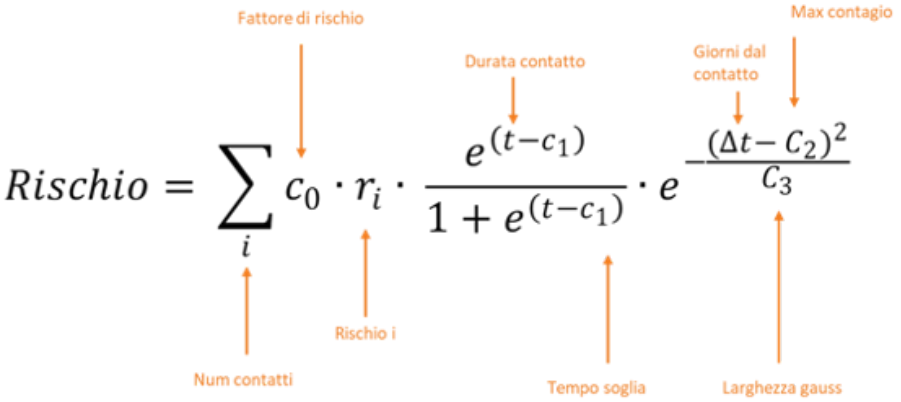
È opportuno che la soluzione tecnologica, anche tramite algoritmi di post-processing dei dati anonimi e crittografati, possa ricostruire con adeguata precisione il "grafo sociale" delle interazioni rilevanti ai fini epidemiologici. A titolo esemplificativo, nel grafico qui sotto, il soggetto infetto (ego) è il triangolo centrale blu; i cerchi rappresentano i singoli contatti, i quadrati rappresentano i gruppi di contatti (la dimensione di ciascun gruppo è indicata). I colori rappresentano le categorie sociali degli incontri (rosso = casa, ciano = lavoro / scuola, giallo = viaggio, rosa = altro). Le maggiori dimensioni dei simboli rappresentano una durata dei contatti più lunga, mentre una maggiore vicinanza all'individuo indica che il contatto è più frequente.



Fonte: Matt J Keeling et al., The Efficacy of Contact Tracing for the Containment of the 2019 Novel Coronavirus (COVID-19), medRxiv doi: https://doi.org/10.1101/2020.02.14.20023036

Va segnalato che, sulla base degli attuali vincoli tecnologici su alcuni tipi di device, in particolare quelli basati su sistema operativo iOS, il solo tracing di prossimità tramite Bluetooth rischia di non massimizzare la probabilità di identificare tutti i contatti, in quanto potrebbe non riuscire a intercettare i segnali provenienti da device dove le funzionalità Bluetooth non operano in modo coerente agli scopi dell'applicazione. Si ritiene quindi opportuno non escludere a priori la possibilità che, sotto condizione di opt-in informato e consapevole, la soluzione tecnologica da implementare possa trattare alcune puntuali e limitate informazioni geolocalizzate, non orientate a ricostruire i percorsi bensì circoscritte a specifici luoghi di potenziale contagio, specie se ad alta densità e frequenza di contatti, in quanto non tutti i contatti possibili potrebbero disporre di device (a causa di una minore penetrazione degli smartphone, specie tra la popolazione anziana) o di app installata (minore adozione/compliance da parte della popolazione). Nell'ipotesi in cui si ritenesse di utilizzare le funzionalità di geolocalizzazione dei dispositivi ancorché in ipotesi limitate occorrerebbe, ovviamente, rivedere le considerazioni sulla natura anonima dei dati trattati non risultando più possibile fare affidamento sull'effettivo anonimato.

Inoltre potrebbero essersi verificati casi di contagio ambientale e quindi potrebbe essere richiesto un intervento di sanitizzazione dei luoghi/locali. Potrebbe essere perciò giudicato opportuno che la soluzione possa conservare, oltre alla lista dei contatti di prossimità, anche un *timestamp* e una limitata cronologia delle geo-localizzazioni per i 14-21 giorni precedenti, ma la raccolta di tali dati, anche previo opt-in dell'utente, va attentamente valutata sulla base dei rischi di re-identificazione che essa comporta, in quanto l'uso della posizione vanifica - de facto - ogni forma di approccio autenticamente privacy-preserving e *può rendere più complessa e meno efficace la strategia di comunicazione pubblica e di acquisizione di utenti che volontariamente usano la suddetta app*. Si nota al riguardo che il Parlamento tedesco ha recentemente negato la possibilità di utilizzare informazioni GPS per applicazioni di contact tracing, approvando una proposta di legge in tal senso il 27 Marzo 2020.
La probabilità di contagio viene normalmente calcolata sulla base di un modello che tiene conto di durata del contatto, dei giorni trascorsi dal contatto e dal numero di questi contatti. I parametri numerici (nello schema qui sotto, indicati con c0…c3) vengono inizialmente stimati partendo dai dati presenti nella letteratura scientifica e vengono successivamente aggiornati man mano che il sistema consente di apprendere i dettagli del meccanismo di diffusione. Qui sotto si propone, a titolo esemplificativo, una forma generale e sintetica del metodo di calcolo del rischio di contagio:



Nella soluzione proposta dal consorzio europeo i dati vengono normalmente conservati solo sul device dell'utente. A seconda degli obiettivi del servizio, alcuni dati aggregati e crittografati possono eventualmente essere periodicamente salvati su un database protetto, per limitare i rischi di perdita o danneggiamento del device e dei relativi dati di contatto. Limitatamente ai casi verificati di contagio, tali dati potranno essere messi in condivisione con le autorità sanitarie per i necessari interventi di contenimento e prevenzione.

I dati acquisiti e il rischio calcolato possono essere resi accessibili in modo anonimo alle autorità sanitarie, che possono leggere i dati di rischio ed aggiornare lo stato di una persona (negativo o positivo al test). Il rischio calcolato per il singolo utilizzatore è in funzione dei dati degli altri utilizzatori. Se una persona risulta positiva al test, il rischio di ogni altra persona con la quale questa sia venuta in contatto viene aggiornato secondo una precisa procedura di "alerting". Per esempio, se una persona con la quale si ha avuto un contatto 5 giorni prima si rivela positiva, il rischio di contagio viene aggiornato sul suo cellulare. Ciascuno riceve le informazioni sul proprio stato di rischio, non su quello di altri. I cittadini possono venire informati in tempo reale e possono spontaneamente adottare misure cautelative (isolamento volontario) nei confronti delle persone più vicine. Le autorità sanitarie locali possono così disporre di uno strumento importante per concentrare i test sulle persone che hanno realmente avuto contatti a rischio contagio.

Più in dettaglio, ai fini di poter convergere con il modello di *digital contact tracing* proposto dal consorzio europeo PEPP-PT, il funzionamento desiderato della soluzione di *contact tracing* può essere sinteticamente così descritto:

1) Invio di un codice identificativo anonimo.

Ogni device abilitato trasmette un identificatore (ID) temporaneamente valido, autenticato e anonimo che non è collegato né a un utente né a un numero di telefono. La prossimità tra

telefoni di altri utenti del sistema viene stimata misurando i segnali radio emessi dal device (Bluetooth, ecc.) utilizzando algoritmi testati e calibrati.

2) Registrazione della cronologia di prossimità.

Quando il device “A” si trova in prossimità epidemiologicamente rilevante del device “B” per un periodo di tempo epidemiologicamente sufficiente, come determinato dalle misurazioni empiriche e dall’euristica medica, l'ID anonimo del telefono B viene registrato nella cronologia di prossimità crittografata memorizzata localmente sul telefono A (e viceversa). Nel modello proposto da PEPP-PT, nessuna geo-localizzazione, nessuna informazione personale, nessun numero di telefono o altri dati vengono registrati, così da non consentire in alcun modo l'identificazione dell'utente. Questa cronologia di contatti di prossimità anonimi non può essere visualizzata da nessuno, nemmeno dall'utente del telefono “A”. Gli eventi più vecchi nella cronologia di prossimità vengono progressivamente eliminati quando diventano epidemiologicamente non importanti (p.es. dopo 21 giorni)

3) Utilizzo della cronologia di prossimità: due modalità operative.

Modalità 1

Se un utente non viene testato o è risultato negativo, la cronologia della prossimità anonima rimane crittografata sul telefono dell'utente e non può essere visualizzata o trasmessa da nessuno, nemmeno dalle autorità sanitarie. In qualsiasi momento, viene salvata solo la cronologia di prossimità che potrebbe essere rilevante per la trasmissione del virus e la cronologia precedente viene continuamente eliminata.

Modalità 2

Nel modello proposto da PEPP-PT, se è stato confermato che l'utente del telefono A è SARS-CoV-2 positivo, le autorità sanitarie contatteranno l'utente A e forniranno all'utente una chiave speciale crittografata, così da garantire che nessun potenziale malware possa inserire informazioni errate sull'infezione nel sistema. L'utente utilizza questa chiave speciale per fornire volontariamente informazioni al servizio sanitario nazionale che consente la notifica di app registrate nella cronologia di prossimità e quindi potenzialmente infette. Poiché questa cronologia contiene identificatori anonimi, nessuna delle due persone può essere a conoscenza dell'identità dell'altra.

4) Operazione di servizio sanitario dipendente dal paese e/o dalla regione.

Gli ID anonimi contengono meccanismi crittografici per identificare il paese e/o la regione di ogni app che utilizza il sistema. Utilizzando tali informazioni, gli ID anonimi vengono gestiti in modo specifico per paese.

Modalità 1
Se entrambi gli ID anonimi del telefono A e B provengono dallo stesso paese, l'ID anonimo della parte potenzialmente infetta può essere contrassegnato, in modo che quando l'app di questa parte chiede informazioni sul suo stato, l'app verrà informata della possibile esposizione.

Modalità 2

Se un ID anonimo del telefono B viene identificato come associato a un altro paese diverso dal telefono A, le informazioni associate all'ID anonimo del telefono B vengono trasmesse al servizio sanitario nazionale dell'altro paese. Questa trasmissione è completamente crittografata e firmata digitalmente. L'ulteriore elaborazione viene eseguita dal servizio sanitario nazionale o locale del paese/regione che ha emesso l'app.

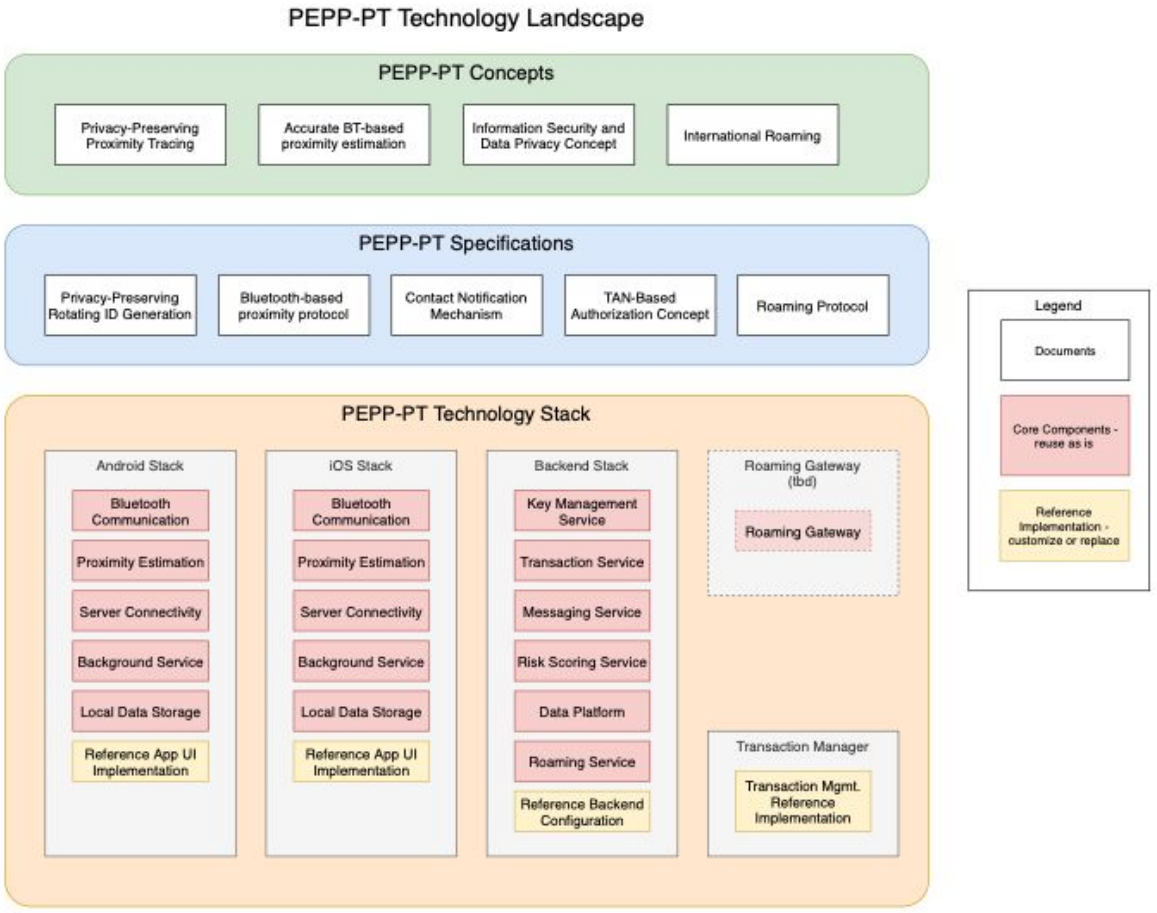
5) Elaborazione sanitaria

Il processo su come informare e gestire i contatti esposti può essere definito Paese per Paese, in modo tale da garantire comunque l'interoperabilità dei processi tra le diverse autorità sanitarie locali.

6) Informazioni e infrastrutture

Tutte le procedure, i meccanismi, gli standard e i codici del sistema vanno costantemente monitorati dal team di sicurezza. Parallelamente, le agenzie nazionali per la sicurezza informatica e le agenzie nazionali per la protezione dei dati controllano regolarmente tutte le linee di codice e le validano dal punto di vista della cybersecurity. Tutto ciò che viene rilasciato al pubblico viene controllato per prevenire effetti indesiderati nelle procedure o nel codice.

Lo schema dell'architettura tecnologica proposta dal progetto PEPP-PT è riportato nella figura seguente, che riprende i concetti, le specifiche di alto livello e la struttura degli stack tecnologici sopra sinteticamente descritti.



Il processo di valutazione

Le attività del Gruppo di Lavoro data-driven per l'emergenza COVID-19 sono state introdotte da una *fast call for contribution* della durata di tre giorni (dal 24 al 26 Marzo), nell'ambito di una iniziativa interministeriale denominata Innova per l'Italia, promossa dal Ministero dello Sviluppo Economico, dal Ministero dell'Università e della Ricerca, dal Ministero per l'Innovazione Tecnologica e la digitalizzazione, dal Ministero della Salute.

Il sottogruppo di lavoro 'Tecnologie per l'emergenza' si è dedicato all'individuazione delle tecnologie per l'identificazione dei casi di potenziale contagio (*contact-tracing*),

immediatamente utilizzabili per governare l'emergenza epidemica ed eventualmente migliorabili con modifiche di facile e rapida realizzazione.[3]

Alla chiusura della *call for contribution*, il processo generale finalizzato all'individuazione delle proposte è stato articolato in cinque passaggi. In particolare:

1. creazione di una griglia di riferimento contenente i requisiti minimi indispensabili per selezionare le soluzioni tecnologiche;
2. uso di tale griglia per la selezione delle proposte da sottoporre a caratterizzazione tecnica da parte degli esperti membri del sottogruppo;
3. verifica delle soluzioni tecnologiche con riferimento alla normativa vigente in particolare in materia di privacy;
4. elaborazione di un documento di sintesi contenente la descrizione delle caratteristiche delle proposte tecnicamente meglio rispondenti all'immediato obiettivo di rispondere all'emergenza epidemica;
5. validazione del documento degli esperti tecnici da parte dei valutatori indicati nel DM del Ministro per l'innovazione tecnologica e la digitalizzazione del 31 marzo 2020

All'attenzione di componenti del sottogruppo 'Tecnologie per il governo dell'emergenza' sono pervenute in esame 319 proposte. La disamina, volta alla selezione delle proposte tecnicamente più rispondenti al bisogno di contribuire tempestivamente al governo dell'emergenza, è stata articolata in tre fasi successive. In particolare:

1. Screening generale, che ha consentito l'individuazione di 15 soluzioni rispondenti ai requisiti tecnici minimi indispensabili;
2. Caratterizzazione analitica, che ha portato alla selezione di una *short list* di 5 soluzioni tecnologiche target, tecnicamente pronte per l'uso di *contact tracing;*
3. Intervista tecnica effettuata sulla *short list* delle 5 soluzioni target, per la definizione di quelle tra queste 5 che offrissero che rispettassero nel miglior modo possibile il maggior numero di criteri definiti.

La fase 1 di screening generale è stata svolta da 5 esaminatori, sulla base di una scheda di analisi appositamente studiata e redatta dai tecnici del sottogruppo di lavoro prima della disamina delle proposte. I criteri presi come riferimento sono rappresentati in tabella 1 e sono stati considerati ciascuno secondo un valore di sufficienza (1) o insufficienza (0). Tutte le proposte che, in corso di disamina, hanno ottenuto un punteggio complessivo di tutti i criteri inferiore a 5, non sono passate alla fase 2 di caratterizzazione analitica.

[3] Le valutazioni sono state effettuate da un team composto dalla seguenti persone: Carlo Alberto Carnevale Maffè, Ciro Cattuto, Leonardo Favario, Andrea Nicolini, Alberto E. Tozzi.

Tabella 1.

	Criteri di screening	**Valore**
A	L'applicazione svolge **la funzione di digital contact tracing**?	1=si
B	**Il proponente** è una Pubblica Amministrazione, un'azienda pubblica o privata, ente o centro di ricerca pubblico o privato, associazione (che possa interagire con associati in grado di rispondere a queste esigenze), cooperativa, consorzio, fondazione o istituto?	1=si
C	La soluzione proposta risulta **concreta, già realizzata o disponibile** per l'implementazione in tempi brevi e compatibili con l'emergenza?	1=si
D	**L'approccio tecnico di rilevazione della prossimità** fisica avviene a mezzo di comunicazione diretta fra i dispositivi (ad esempio via tecnologia radio Bluetooth) ed è indipendente da informazioni altrimenti ottenute sulla posizione degli utenti nello spazio (geo-localizzazione, GPS, SSID WiFi, cella della rete mobile, etc.)?	1=si
E	**Disponibilità della soluzione tecnologica e tempi per l'attivazione dei servizi per il deployment** *(valuta la velocità con la quale la tecnologia può avere impatto; assegnare il valore 1 se si stima che i servizi possano essere attivi indicativamente entro 15 giorni, 0 altrimenti. Considerare anche l'adattamento di applicazione sviluppata per altri scopi).*	1=si
F	**Aspetti tecnici di rilevazione della prossimità** (*valuta la bontà della soluzione in termini di accuratezza nella rilevazione di parametri a valenza epidemiologica (es. risoluzione della distanza, del momento di inizio e della durata dei contatti) assegnare il valore 1 se la soluzione proposta consente misure di prossimità device-to-device passive a corto raggio e calibrazione della strategia di proximity detection, 0 altrimenti).*	1=si
G	**Aspetti tecnologici / prestazionali e di scalabilità** *(1 se la soluzione è basata su codice FLOSS, architettura scalabile e adeguate soluzioni di crittografia dei dati, protezione della privacy e data minimisation).*	1=si

La fase 2 di caratterizzazione analitica è stata svolta da 5 esaminatori con l'utilizzo dei seguenti indicatori e criteri, suddivisi in tre categorie:

Tecnologia

- Soluzione FLOSS: tutto il codice sorgente della soluzione è coperto da licenze FLOSS tra loro compatibili ed è disponibile all'interno di un repositorio pubblico completo di documentazione.
- La soluzione non ha dipendenze (software e/o architetturali) di natura proprietaria che potrebbero costituire lock-in.
- La soluzione tecnica consente misure di prossimità device-to-device passive a corto raggio.
- Calibrazione della strategia di proximity detection a corto raggio (per tenere conto delle differenze hardware tra diversi smartphones).
- Approccio massimamente distribuito: minimizzazione dei dati di contatto registrati in modo centralizzato ai soli dati strettamente necessari per le misure di contact tracing, testing e contenimento.
- Possibilità di deployment internazionale, con interoperabilità privacy-preserving di server nazionali (feature di "roaming").
- Facilità di raccordo della soluzione tecnica con il processo epidemiologico e clinico di contact tracing.
- Campionamento temporale delle relazioni di prossimità a frequenza sufficientemente alta, passivamente attivato.
- Strategie di power saving che riducono l'uso batteria e risultante churn degli utenti.
- Informazioni sul contesto dei contatti (e.g., contatto "indoors" oppure "outdoors").
- Architettura elasticamente scalabile e multi-tenant (numero limitato di interazioni con il backend, architettura backend non monolitica).
- Tecnologia privacy-preserving, con opzioni tramite consenso informato: assenza di soggetti privati con accesso ai dati individuali.
- Uso di crittografia *state of the art.*
- Possibilità di cancellazione dei propri dati locali/remoti.
- Basso debito tecnico (complessità di manutenzione, deploy, gestione)

PM & deployment

- App già rilasciata negli store, numero di download e feedback raccolti.
- Livello di testing raggiunto (maturità codebase).
- Facilità d'uso e incentivi all'adozione.
- Base di utenti già esistente e/o possibilità di refactoring della soluzione già adottata.
- Approccio internazionale. Consente scambio di best practices, testing distribuito su popolazione più vasta, riduzione di costi e rischi.

- Approccio tecnico che fa leva su esperienza di gruppi di ricerca internazionalmente riconosciuti in contact tracing con mezzi digitali. Integrazione con sistemi sanitari locali e medici di base.

Data analytics

- Capacità della soluzione di rilevare parametri di riconosciuta valenza epidemiologica per un patogeno a trasmissione aerea: risoluzione di interazioni di prossimità a corto raggio, risoluzione temporale di contatti individuali.
- Uso di ID robusto per interoperabilità con altri database in caso di decriptazione.
- Integrazione con altre informazioni da questionario contestuale integrato.
- Strategia di analisi dei dati con approccio privacy-enhancing, guidata dallo stato dell'arte della letteratura scientifica rilevante su contact tracing, outbreak investigation, high-resolution contact networks.
- Meccanismo di "scoring" del rischio individuale che faccia leva su graph analytics.
- Tecniche di machine learning a sostegno del contact tracing e dello scoring del rischio.
- Disponibilità di una piattaforma di analisi dati matura / già testata / integrata con il back end dell'applicazione.

User Experience / User Interface

- Approccio al design del progetto incentrato sull'utente finale (ricerca utenti, interaction design, visual design, architettura delle informazioni/contenuti).
- Design focalizzato su usabilità e accessibilità.

La fase 3 di intervista tecnica ai proponenti rientrati in *short list* ha permesso di approfondire alcuni aspetti tra cui:

- maturità/stage della soluzione;
- sicurezza/affidabilità;
- tecnologia di *contact tracing* utilizzata;
- approccio allo sviluppo *software*;
- architettura e approcci al *deployment*;
- analisi di potenziale *lock-in* (*software*, infrastrutturale);
- presenza di componenti critiche non rilasciabili con licenze FLOSS;
- composizione del team, delle partnership e dei ruoli;
- analisi della roadmap.

Intervista 1 - ProteggInsieme

Dall'intervista a Whatif srl, gruppo proponente della soluzione "ProteggInsieme", si evince che l'offerta è stata interamente costruita partendo dalla soluzione proposta dal Government Digital Services team di Singapore e basata sul protocollo *Bluetrace*[4]. In tal senso, lo stato di ProteggInsieme in data odierna è molto preliminare (*concept*) ovvero non esiste una versione funzionante e testabile di questo prodotto e questo è imputabile al fatto che il codice sorgente del *software* sviluppato dal team di Singapore non sia ancora stato reso disponibile a terzi. Inoltre, siccome *Bluetrace* è un protocollo basato sulla tecnologia Bluetooth, si ritiene opportuno sottolineare che il team di ProteggInsieme non ha un track record di esperienze pregresse per quanto riguarda questa specifica tecnologia ma potrebbe appoggiarsi alla propria rete di partner per ovviare a ciò. Infine, l'intervista ha reso evidente che la proposta ProteggInsieme necessita di ulteriore sviluppo su diversi fronti per essere pronta a rispondere pienamente alla sfida del digital contact tracing.

Intervista 2 - TrackMyWay

La soluzione "TrackMyWay", proposta da Antares Vision spa, si basa su un know-how solido del proponente nel mondo del tracking di beni di consumo (come, ad esempio, tracking di spedizioni di farmaci). In tal senso, la soluzione è fortemente incentrata sulle tecnologie di backend di proprietà di Antares Vision utili alla ricostruzione del grafo dei contatti per ogni nodo. Nel dettaglio, la proposta prevede di raccogliere una serie di informazioni attraverso un'applicazione mobile (quali, ad esempio, le coordinate GPS e l'eventuale contatto con altri device rilevato tramite Bluetooth) le quali dovranno essere successivamente inviate al backend costituito dalle summenzionate tecnologie. Ad ogni modo, dall'intervista non sono risultate chiare le scelte riguardanti le misure utili a minimizzare la quantità di informazioni da prelevare e successivamente trasferire al backend, le strategie da adottare per la gestione delle diverse risposte tra i vari dispositivi Bluetooth e le possibili modalità di rilevazione di eventi iOS-to-iOS. Inoltre, sebbene il team abbia esperienza comprovata nel campo del *tracking* digitale di oggetti in movimento tramite tecnologia GPS non vi è un track record significativo nel campo del *digital contact tracing.* Infine, l'architettura proposta risulta avere una natura centralizzata il che rappresenta un possibile problema in ottica di messa in esercizio su scala nazionale.

[4] BlueTrace: https://bluetrace.io/

Intervista 3 - CovidApp

La soluzione denominata "CovidApp" è stata proposta da un team di sviluppatori indipendenti. Dall'intervista con il team si evince che il problema sia stato analizzato in modo approfondito e molti dei possibili scenari che potrebbero presentarsi anche su scala nazionale sono stati esaminati nel dettaglio. CovidApp è quindi una soluzione basata su un'applicazione mobile per la gestione del *contact tracing* attraverso la tecnologia *Bluetooth Low Energy*. In primis, l'applicazione raccoglie i dati relativi ai contatti registrati che vengono registrati all'interno del device. Successivamente, l'applicazione invia i dati raccolti al backend -ogni 4 ore- il quale li elabora per costruire il grafo dei contatti. In quest'ottica, risulta degno di nota l'approccio utilizzato per la rilevazione dei contatti tra dispositivi con sistema operativo iOS che prevede di sfruttare la triangolazione con altri device con sistema operativo Android e successiva ricostruzione del grafo di prossimità. Un possibile svantaggio di questa soluzione è che numerose informazioni devono essere inviate al backend diverse volte al giorno il che non solo aumenta i requisiti in termini di risorse computazionali e di memorizzazione, ma potrebbe costituire un problema di scalabilità dell'intera architettura. Si noti, inoltre, che la rappresentazione del grafo di prossimità in modo centralizzato presso il backend, in cui ogni nodo ed interazione sono rappresentati indipendentemente dall'essere identificati rispettivamente come casi o come interazioni a rischio (ovvero a prescindere dal processo di *contact tracing*), comporta rischi di data protection e privacy più alti di approcci distribuiti che sono ugualmente efficaci per le strategie di *contact tracing digitale.*

Successivamente, l'intervista ha permesso di dettagliare il processo di alerting previsto da questa soluzione. Questo offre alle autorità sanitarie, a seguito della rilevazione di un caso positivo, la possibilità di attivare automaticamente e immediatamente l'alert. Inoltre, quest'ultimo è garantito essere del tutto anonimo in quanto non è necessario disporre del numero di cellulare dell'utente né del suo identificativo personale. Si noti come questa caratteristica si differenzia notevolmente dal modello PEPP-PT, che invece richiede obbligatoriamente -per attivare il processo di alerting su log dei contatti- il consenso e la collaborazione attiva da parte dell'utente riconosciuto come positivo che per procedere dovrà immettere un codice TAN sul proprio device.

Infine, durante l'intervista è stato possibile assistere ad una dimostrazione in tempo reale del prodotto che è attualmente in fase di test privato tra i membri del team.

Intervista 4 - Immuni

La proposta denominata “Immuni” è stata formulata da un pool composto da Bending Spoons, Jakala, GeoUniq e Centro Medico Santagostino. Ognuno di questi attori ha partecipato alla realizzazione del prototipo presentato.

L’intervista ha permesso di conoscere la genesi del progetto e capirne alcune scelte architetturali. Nel dettaglio, il concetto alla base di Immuni si avvicina molto a quello proposto nel protocollo BlueTrace presentato dal team di Singapore. Infatti, Immuni sfrutta la tecnologia Bluetooth Low Energy (BLE) per riconoscere le interazioni tra due device. Di conseguenza, ognuno di questi eventi è salvato nella memoria del dispositivo in modalità cifrata. Si noti che queste informazioni non lasciano mai il dispositivo a meno che il proprietario sia diagnosticato positivo al virus. In tal caso, le informazioni relative a tutti gli eventi di contatto precedentemente registrate dal dispositivo vengono inviate al backend dopo esplicita autorizzazione del proprietario. Solo a questo punto sarà possibile ricostruire a ritroso la catena di contatti e, laddove necessario, la piattaforma potrà inviare una notifica a tutti i dispositivi interessati da eventi di contatto.

Per quanto riguarda la copertura dei dispositivi mobile, il team afferma di poter tracciare correttamente il 94% dei contatti di tipo Android-Android e iOS-Android. Invece, per quanto riguarda la rilevazione degli eventi di contatto tra due device con sistema operativo iOS, il team ha proposto due possibili alternative: la prima consiste in un artificio software mentre la seconda consiste nell’utilizzo del segnale GPS. Questa seconda strategia risulta essere particolarmente accurata grazie ad una libreria software sviluppata da GeoUniq. Si noti, però, che l’utilizzo di questa libreria proprietaria porterebbe ad un lock-in software.

Per quanto concerne il back-end, la soluzione si compone di componenti FLOSS e attualmente l’architettura di test risulta essere funzionante all’interno dell’infrastruttura di Google Cloud ma, siccome non sono stati utilizzati componenti proprietarie, si esclude il rischio lock-in.

Infine, l’intervista ha permesso di conoscere il team il quale è parso solido, con esperienza pregressa sia nel roll-out di applicazioni mobile su larga scala che di gestione di progetti software complessi anche in modalità FLOSS. Anche gli aspetti epidemiologici dell’applicazione sono stati messi a punto grazie alla partnership con il Centro Medico Santagostino.

Si noti in ultima istanza che il team ha già aderito e collabora attivamente con il Consorzio Europeo PEPP-PT. Quest’ultimo è un fattore positivo per quanto riguarda la capacità di lavorare a livello paneuropeo e nell’ottica di implementare in breve tempo una soluzione europea condivisa.

Intervista 5 - SafeTogether

La proposta SafeTogether, avanzata da Microsoft srl, ha lo scopo di realizzare una piattaforma versatile di raccolta dati relativi alla pandemia in corso. Dall'intervista con il team proponente si evince che la soluzione SafeTogether si trova in una fase molto preliminare di realizzazione (*concept*). Infatti ad oggi non esiste una vera e propria soluzione utilizzabile ma vi sono esclusivamente degli scenari di possibile utilizzo e la roadmap di progetto stima circa 4/5 settimane per la realizzazione di un oggetto preliminare da testare sul campo. Nello specifico, la proposta SafeTogether contiene diverse componenti infrastrutturali e di backend con la finalità di facilitare la raccolta e le operazioni di analisi dei dati ma non ha un frontend applicativo il che rende difficile immaginare un caso reale di utilizzo. Per quanto riguarda l'esperienza diretta con la pandemia attualmente in corso, il team di SafeTogether ha fatto presente che il modello da loro teorizzato segue quanto messo in opera dal GDS team di Singapore (TraceTogether).

Intervista extra - COMBAT

Al fine di approfondire anche alcune proposte che non hanno dichiarato esplicitamente di utilizzare le tecnologie di *digital contact tracing* più comuni, il gruppo di valutazione ha ritenuto opportuno procedere con l'intervista tecnica a Telecom Italia Spa in qualità di proponente della soluzione "COMBAT".

L'intervista ha permesso di chiarire che il framework "COMBAT" si compone di due soluzioni complementari tra di loro. La prima è prettamente rivolta allo sfruttamento di dati di celle telefoniche già disponibili al gruppo proponente mentre la seconda è basata su un'applicazione mobile.
Per quanto concerne la prima soluzione, la proposta prevede di sfruttare il database di informazioni riguardanti le celle telefoniche ed estrarne le informazioni utili per il *tracing*. Questo tipo di approccio è del tutto trasparente nei confronti dell'utente finale al quale, però, non verrebbe offerta esplicitamente la possibilità per un eventuale opt-out. Inoltre, attualmente l'accuratezza di questo approccio per la finalità del *tracing* non è paragonabile a quella offerta da altre tecnologie.
Il secondo approccio, invece, prevede di sfruttare un'applicazione mobile da realizzare *ex novo*. Questa applicazione potrebbe colmare il gap lasciato dalla soluzione presentata precedentemente in quanto consentirebbe di ottenere una risoluzione intra-cella maggiore e fornire questi dati al backend per una ricostruzione del grafo di tracing ex post. Si noti, però, che attualmente la seconda soluzione è in fase molto preliminare di realizzazione (*concept)* e quindi non è stato possibile valutarne la maturità. Infine, la roadmap dichiarata per la messa in opera della seconda soluzione è stata stimata in 4 settimane.

Caratteristiche tecniche delle soluzioni

Al termine delle tre fasi del processo di *selezione, caratterizzazione e valutazione delle proposte* è stata realizzata una tabella sinottica delle soluzioni ritenute maggiormente affidabili, per illustrarne le principali caratteristiche tecniche, i punti di forza e le possibili criticità.

Nome soluzione	**Immuni**	**CovidApp**
Tecnologia	App nativa, iOS (Swift) e Android (Kotlin).	App nativa, iOS e Android.
Program Management	Team con esperienza nel roll-out di applicazioni mobile verso milioni di utenti. Team include competenze verticali in sviluppo app mobile, data analytics, aspetti epidemiologici, geolocalizzazione. Prototipo dell'applicazione realizzato e attualmente in fase di testing privato intra team di sviluppo.	Team distribuito creato ad hoc. Prototipo dell'applicazione realizzato e attualmente in fase di testing privato intra team di sviluppo.
Punti di forza	Integra la soluzione "PEPP-PT". Architettura fortemente decentralizzata. Ampio spettro di possibilità per livelli di privacy e opt-in. Le informazioni restano cifrate sull'edge e vengono rimosse	Rilevazione del contatto iOS-to-iOS tramite grafo di prossimità elaborato nel backend come triangolazione tra contatti Android.

	progressivamente ogni 14/21 giorni. Alta scalabilità backend.	
Criticità	Rilevazione del contatto iOS-to-iOS non gestita	Architettura centralizzata: rappresentazione centralizzata del grafo di prossimità per tutti gli utenti, indipendentemente dalla diagnosi, con continuità temporale. Vincoli più forti di scalabilità e performance del backend. La rappresentazione centralizzata del grafo di prossimità nel backend implica rischi maggiori di data protection e privacy.

Realizzazione e sperimentazione

Per accompagnare l'uscita dal *lockdown* del Paese, è vitale prevedere un processo particolarmente attento ancorché veloce di validazione e messa in esercizio della soluzione prescelta che garantisca il raggiungimento degli obiettivi previsti.

Alla luce di queste considerazioni, il processo di implementazione deve essere ridondato e deve basarsi su almeno 2 soluzioni, al fine di avere la certezza di poter disporre di almeno una soluzione da mettere in campo qualora, in fase di sperimentazione concreta, una delle opzioni prescelte si rivelasse per qualunque motivo incapace di offrire le funzionalità e/o i livelli prestazionali richiesti. Per questo motivo, si propone di articolare il processo di implementazione della soluzione di *contact tracing* lungo **percorsi paralleli** in accordo al seguente modello:

a. Effettuare un approfondito *assessment* di sicurezza sull'intero codice sorgente, dell'architettura e del sistema delle soluzioni individuate, incluso risk assessment e threat modeling (a cura del comparto di *intelligence*). Inoltre sarebbe opportuno condividere il codice sorgente con la comunità scientifica dell'ambito cyber

nell'ottica di avere delle review dal maggior numero di specialisti del settore possibile.

b. Effettuare una fase di *test* in campo per ciascuna soluzione preselezionata in diverse aree circoscritte del territorio (per esempio, alcuni territori urbani). Tale test potrà essere condotto su un campione di soggetti (per esempio, le forze dell'ordine e gli operatori della protezione civile) che, muovendosi sul territorio nonostante le misure restrittive degli spostamenti ancora in atto, possono già verificare il corretto funzionamento di ciascuna soluzione.

   Perché ciò avvenga, è necessario in via preliminare completare alcuni passaggi:

   i. stabilire i necessari protocolli d'uso dell'applicazione (da parte del personale medico-sanitario, delle forze di pubblica sicurezza e dei cittadini/tester);
   ii. migliorare il funzionamento dell'applicazione sulla base delle esigenze riscontrate, integrando eventuali funzionalità per meglio rispondere alle richieste emerse in fase di test;
   iii. definire il necessario coordinamento fra enti territoriali, ISS e Protezione Civile per l'uso dell'applicazione.

Questa fase di test in parallelo delle soluzioni candidate dovrebbe iniziare subito dopo la fase di validazione e scelta delle soluzioni tecnologiche da parte delle Autorità di Governo e durare indicativamente 10 giorni, così da rendere disponibile l'applicazione che presenta le migliori prestazioni per l'impiego su larga scala sin dall'inizio del processo di uscita dal *lockdown.*

Inoltre, è necessario che, parallelamente alla messa in esercizio della soluzione tecnologica (fase di test), siano perseguiti i seguenti obiettivi:

1. delineare processi di carattere strategico-organizzativo in ambito sanitario, utili per governare il sistema di controllo dei contagi nel suo complesso e per dar seguito operativamente alle indicazioni che emergeranno dalla disponibilità delle tracciature (come ad esempio la gestione dei potenziali contagiati e il loro isolamento e cura), incluso il programma che sarà messo in campo per la comunicazione e formazione verso il personale sanitario;
2. definire gli aspetti giuridici, e tecnici relativi al tema privacy, etica e sicurezza b*y design*, inclusa la mappa del flusso dei dati, i soggetti che hanno accesso ai dati, e le condizioni di accesso;
3. definire un processo di *governance* che servirà a supervisionare l'esercizio, l'evoluzione e la valutazione del sistema di tracciatura nella sua fase operativa;
4. valutare l'integrazione con le infrastrutture tecnologiche esistenti per la gestione delle basi di dati centralizzate.

Per la gestione operativa a regime della soluzione di *contact tracing* sono necessarie sei componenti chiave:

1. Una autorità pubblica che rivesta il ruolo di *Driver* dell'esecuzione dell'intero progetto, preoccupandosi di curare la messa in opera di tutte le attività necessarie e coessenziali affinchè il *contact tracing* sia utilmente impiegato su scala nazionale (training dei medici, supporto tecnico agli utilizzatori, etc.). È fortemente raccomandabile che sia individuata una figura di *Program manager* con mandato esecutivo, in particolare per la fase iniziale del progetto.
2. Un team di sviluppo interdisciplinare che riunisca competenze tecnologiche e di sanità pubblica con una forte leadership e con le competenze digitali necessarie per guidare lo sviluppo e la manutenzione della soluzione, collaborando anche con gli stakeholder europei (queste caratteristiche andrebbero ricercate in un soggetto privato o in un consorzio di soggetti privati che supportino lo sviluppo del codice delle componenti applicative della soluzione individuata).
3. Un soggetto governativo in grado di gestire, mediante un fornitore di servizi tecnologici a controllo pubblico, l'infrastruttura tecnologica del servizio di contact tracing, garantendo massima sicurezza ed un'elevata affidabilità del servizio.
4. Una *governance* delle informazioni chiara e trasparente affidata all'autorità sanitaria nazionale e alla protezione civile.
5. Una diffusa e capillare campagna di *nudging*, comunicazione e informazione della cittadinanza, al fine di incoraggiare una partecipazione attiva e consapevole, guidata dalla Presidenza del Consiglio per massima autorevolezza.
6. La vigilanza sull'intero processo da parte della pubblica sicurezza e del comparto di *intelligence*.

La tabella seguente riassume a titolo puramente preliminare un'ipotesi di suddivisione delle competenze tra gli attori coinvolti nella realizzazione e gestione del servizio di *contact tracing*.

	Program Manager	Team di sviluppo	Gestore del servizio tecnologico	Autorità sanitaria	GPDP	PCM	DPC
Definizione Roadmap	A	R	R	C	I	C	I
Sviluppo e manutenzione della soluzione tecnologica	R	A	C	C			I
Gestione del sistema di contact tracing	R	C	A	I			C
Garantire anonimato dei dati trasmessi	R	R	A				
Gestione clinica sanitaria e attivare il contact tracing	C			RA			
Vigilanza sulla sicurezza	R	R	R			A	I
Vigilanza sulla privacy	R	R	R		A		
Campagna di comunicazione	R			C		A	I

Legenda:

- **Responsible (R)**: è il soggetto che esegue e assegna l'attività
- **Accountable (A)**: è il soggetto che ha la responsabilità sul risultato dell'attività.
- **Consulted (C)**: è soggetto che aiuta e collabora con il Responsible per l'esecuzione dell'attività.
- **Informed (I)**: è soggetto che deve essere informato al momento dell'esecuzione dell'attività.

Grande importanza assume a questo riguardo una *roadmap* di sviluppo agile che preveda una serie di rilasci scaglionati nel tempo dell'utilizzo della tecnologia, il cui proficuo impiego nel contenimento dell'epidemia e nella prevenzione di nuovi contagi richiede tempo e risorse dedicate.

Per la stima preliminare dei tempi e dei costi di sviluppo, test e roll-out nazionale, si può dividere il programma complessivo in tre fasi:

1. **Alpha** (prototipo per i primi test funzionali) + **Beta** (fase di perfezionamento e test sul campo in contesti/zone delimitati). Questa fase può richiedere circa 3 settimane di lavoro con costi derivanti principalmente dal team tecnico impegnato sui due prototipi che saranno scelti per limitare i rischi.

2. **Roll-Out su scala nazionale**. Estensione progressiva dell'adozione a tutta Italia. Questa fase può richiedere circa 3-4 settimane con i costi più rilevanti dovuti al programma di comunicazione e ai costi di setup e di progressivo allargamento dell'infrastruttura, in questo caso relativa all'unica soluzione che sarà scelta per l'uso a regime

3. **Gestione software a regime**. Questa è una fase di durata indefinita, durante la quale il sistema viene esercito e progressivamente ampliato e migliorato usando le informazioni acquisite sul campo per affinare la precisione e l'efficacia, aggiungere funzionalità ulteriori di cui - a lancio già avvenuto - si dovesse scoprire l'utilità, nonché garantire la continua integrazione con gli analoghi programmi portati avanti dagli altri paesi europei con i quali si intenderà collaborare.

Per ogni eventuale nuova versione con significative funzionalità aggiuntive, da sviluppare in modalità "agile", si può stimare prudenzialmente un monte-ore di lavoro pari allo sviluppo della versione base.

Per l'operatività immediata su **infrastrutture cloud sicure** e ad altissima affidabilità, la previsione dei costi può dipendere da molti fattori, principalmente rappresentati dal numero di persone che installeranno l'applicazione, dalla frequenza con la quale l'applicazione contatterà il sistema *backend* per aggiornamento dei dati, dalla quantità di persone che dovranno essere allertate perché entrate in contatto con positivi, dalla dimensione dei dati di tracciamento mediamente prodotti da ogni persona. Paragonando con progetti analoghi, è possibile immaginare che il costo complessivo del progetto potrebbe essere, prudenzialmente, al più nell'ordine di qualche milione di euro l'anno.

Le funzionalità software di base qui previste includono il tracciamento contatti basato su Bluetooth LE, il diario clinico, l'interfaccia utente e l'integrazione software in sicurezza con l'infrastruttura cloud, oltre alle funzionalità necessarie per far funzionare il sistema end-to-end. Non sono incluse nelle stime di costi e tempi iniziali altre funzionalità quali la georeferenziazione di alcuni dati o lo sviluppo del sistema di data analytics territoriali e l'integrazione con le basi dati sanitarie regionali e nazionali. Queste estensioni sono da ritenersi necessarie ma andranno valutate e stimate in una fase successiva all'avvio del progetto. Nel caso in cui le autorità decidano di seguire le raccomandazioni del Gruppo di Lavoro, ovvero procedere con due soluzioni in parallelo per le fasi di alpha + beta test, alla stima generale di costi di operatività andrà aggiunto un importo dovuto alla sperimentazione con l'applicazione "piano B", che sarà comunque marginale rispetto al costo totale dell'operazione.

Altri costi che andranno tenuti in considerazione saranno, a titolo esemplificativo e non esaustivo, i costi di comunicazione e pubblicità, i costi di integrazione con eventuali soluzioni internazionali, i costi per i servizi di roaming transfrontaliero del contact tracing e dell'alerting, i costi di sviluppo di dashboard specializzati per specifici scopi istituzionali o medico-sanitari.

Considerazioni sulla sicurezza delle informazioni

Una soluzione applicativa con una diffusione così ampia nella popolazione si presta con elevata probabilità a divenire oggetto di numerosi tentativi di frode e/o attacchi informatici.
Eventuali attività di compromissione potrebbero, ad esempio, essere basate su tecniche di phishing, come creazione di app o di siti "civetta" con loghi o nomi contraffatti che potrebbero essere scambiati per il servizio stesso dagli utenti finali.
E' pertanto di vitale importanza porre la massima attenzione agli aspetti di sicurezza delle informazioni dell'intero sistema di *contact tracing*, al fine di garantire la necessaria resilienza e la continuità operativa dei servizi, anche come contrasto a tentativi esterni di compromissione dei sistemi. Non è stato ad oggi possibile, dato il limitato tempo a disposizione, svolgere un approfondito audit di sicurezza del codice sorgente delle due applicazioni candidate alla fase di sperimentazione. Pertanto si raccomanda fortemente di svolgere quanto prima tale audit, nonché un approfondito *assessment* sui soggetti proponenti e sulle componenti tecnologiche di terze parti utilizzate.
Si raccomanda, altresì, una valutazione del rischio (*risk assessment*) ad ampio raggio dell'intero sistema di *contact tracing* e di tutti i soggetti coinvolti, con particolare riferimento alle differenti ipotesi implementative che potranno essere individuate.
Per questo motivo si rende necessario il coinvolgimento delle autorità preposte alla sicurezza nazionale con specifiche competenze in ambito di *cybersecurity*.
Infine, per garantire una maggiore sicurezza e trasparenza, dopo la verifica eseguita dalle autorità sopra indicate, potrebbe essere opportuno rilasciare pubblicamente il codice sorgente delle applicazioni, in modo che tutta la comunità di esperti in materia di *cybersecurity* a livello nazionale abbia la possibilità di scrutinare il sistema e segnalare eventuali problemi non ancora rilevati.
Tale scelta contribuirebbe, peraltro, ad innalzare il livello di fiducia nel progetto da parte dei cittadini.

La seguente tabella riporta, a titolo puramente indicativo, una preliminare e non esaustiva analisi del rischio (tipologia e livello di rischio associati alla soluzione, unitamente alle possibili mitigazioni), sviluppata in base alla metodologia *STRIDE (vedi legenda)*.

Tipologia	**Rischio**	**Livello**	**Possibile Mitigazione**
Information disclosure / Spoofing	Phishing mediante contraffazioni e diffusione di fake news	Alto	Distribuzione dell'app esclusivamente tramite app store e campagne di informazione
Spoofing	Inquinamento delle liste di contatto	Alto nel caso di CovidApp	Sistema di autenticazione dei client basato su certificati (certificate pinning)
Denial of Service	Attacchi DoS/DDoS agli endpoint backend	Alto	Architettura distribuita, DNS e contromisure anti-DDoS
Denial of Service	Boicottaggio della soluzione sfruttando campagne di disinformazione	Medio	Nudging e campagna di informazione, sorveglianza da parte di AGCOM
Information Disclosure	Exploit del codice o injection di trojan nell'applicazione al fine di raccogliere informazioni sulla posizione GPS, MOBILE, WiFi SSID etc.	Medio	FLOSS e community based, responsible disclosure policy, bug bounty
Elevation of Privilege	Exploit del backend al fine di segnalare possibili falsi contagi seminando panico	Alto	Hardening backend, audit frequenti e analisi logging, SOC
Tampering / Integrità del dato	Alterazione delle informazioni salvate sul device e/o inviate al backend. Renderebbero costruzione del grafo di prossimità impossibile	Medio	Audit e monitoraggio dei sistemi di crittografia e della struttura dati
Non ripudio	Dichiarazione di non aver compiuto una determinata azione (non aver avuto contatti)	Alto	Nudging/comunicazione e consenso informato
Tampering	Switch off del device BLE per non registrare i contatti	Basso	Audit dei log del device ex-post

Legenda:

STRIDE[5] è un processo metodologico che aiuta ad individuare le minacce di sicurezza in un sistema complesso,

- Spoofing (falsificazione di identità): la pretesa di essere qualcos'altro o qualcun altro che non si è.
- Tampering (alterazione dei dati): l'alterazione di qualcosa che si presuppone non sia oggetto di modifica.
- Repudiation (ripudio di una azione): significa dichiarare di non aver fatto qualcosa (indipendentemente dal fatto che sia stato fatto o meno).
- Information Disclosure (divulgazione di informazioni): riguarda l'esposizione delle informazioni a persone non autorizzate alla loro visione.
- Denial of Service (diniego di servizio): sono attacchi designati all'interruzione del servizio.
- Elevation of Privilege (elevazione dei privilegi): avviene quando un programma o un utente è tecnicamente abilitato a fare cose che si presuppone non debba fare.

Privacy

Per le considerazioni sulla protezione dei dati personali e la privacy si fa riferimento alla relazione prodotta dal sottogruppo "Profili giuridici della gestione dei dati connessa all'emergenza".

Conclusioni

Il *contact tracing* o tracciatura dei contatti è una delle azioni di sanità pubblica utilizzate per la prevenzione della diffusione di alcune malattie infettive e rappresenta un elemento importante all'interno di una strategia sostenibile post-emergenza. La sua efficacia è stata ben documentata durante la fase di contenimento della pandemia influenzale del 2009 [3]. In anni più recenti, questo metodo è stato uno strumento prezioso: nel 2014, in seguito all'importazione della malattia da virus Ebola nel Regno Unito [4] e nel 2018 nel caso di monkeypox [5]. I principali vantaggi del *contact tracing* sono che può identificare individui potenzialmente infetti prima che emergano sintomi [1] e, se condotto in modo sufficientemente rapido, può impedire la trasmissione successiva dai casi secondari.

Sulla base di stime recenti per la trasmissione COVID-19, le ricerche empiriche [6] mostrano che per rintracciare almeno l'80% dei contatti delle infezioni rilevate, è necessario prevedere un onere logistico molto elevato, con una media di 36,1 individui (95 percentili: 0-182) tracciati per ogni caso di contagio. Se si rende più larga la definizione di contatto, è possibile ridurre questo onere, ma con un corrispondente aumento del rischio di casi non tracciati; i ricercatori stimano che, per qualsiasi definizione di stretto contatto si voglia adottare, una procedura di *contact tracing* manuale che richieda più di 4 ore di ricerca è probabilmente destinata a generare una diffusione incontrollata dell'infezione. Gli standard di *contact*

[5] Linee guida per la modellazione delle minacce ed individuazione delle azioni di mitigazione conformi ai principi del secure/privacy by design:
https://www.agid.gov.it/it/sicurezza/cert-pa/linee-guida-sviluppo-del-software-sicuro

tracing manuale forniti dall'European Center for Disease Prevention and Control (ECDC) nel marzo 2020 relativamente all'epidemia di COVID-19 indicano tuttavia in 12 ore – con l'utilizzo di 3 risorse di personale specializzato - il tempo medio per ogni operazione di *contact tracing*, con un tasso di successo peraltro insufficiente a identificare tutti i contatti o comunque a ridurre il numero di contatti secondari infettati non identificati e isolati sotto l'unità (e quindi a interrompere la riproduzione epidemica).

L'uso della tecnologia in ambito di *contact tracing* appare promettente e in grado di dare un contributo rilevante per un tracciamento di prossimità molto più efficiente e rapido di quello tradizionale. La tecnologia per il *contact tracing* deve tuttavia essere approcciata in modo molto responsabile ed in linea con i diritti e le libertà fondamentali dei cittadini. Un processo di selezione verso una soluzione tecnica che renda possibile il *contact tracing* tramite *smartphone* ma senza tracciare le persone e/o accedere a dati sensibili e informazioni personali (ad esempio chi sono e dove sono state), è stato di recente avviato a livello europeo da un Consorzio che coinvolge eccellenze nella ricerca scientifica e tecnologica in Europa allo scopo di tracciare solo le relazioni di prossimità a corto raggio che costituiscono un rischio di esposizione e che corrispondono a potenziali catene di trasmissione del virus.

La soluzione paneuropea si basa su tre principi di base, in particolare: 1) è il risultato di un'analisi ben documentata dei benchmark internazionali e di un forte spirito di cooperazione europea; 2) la tecnologia è studiata e selezionata per essere applicabile a livello internazionale, vale a dire interoperabile oltre i confini nazionali; 3) la tecnologia è privacy-preserving e dunque conforme al regolamento generale sulla protezione dei dati (GDPR). Dunque la tecnologia alla base della soluzione europea, rappresenta un contributo importante per consentire il tracciamento della prossimità, anche in modalità transfrontaliera, nel rispetto della privacy, secondo un modello scalabile e aperto che possa essere utilizzato da qualsiasi paese.

Allineandosi a tali principi, questo sottogruppo di lavoro dedicato allo studio delle tecnologie per la gestione dell'emergenza in Italia, ha svolto con rigore metodologico un processo di selezione e valutazione di proposte tecnologiche, rilevate con fast-call di tre giorni dal 24 al 26 marzo u.s. La disamina delle soluzioni è stata articolata su tre livelli consecutivi che, partendo da uno screening generale di tutte le proposte, ha permesso - dopo caratterizzazione analitica e interviste tecniche e organizzative - di giungere all'individuazione di due sole soluzioni tecnologiche, ritenute teoricamente valide per essere testate a scopo di implementazione nell'attuale situazione emergenziale. Si tratta in particolare di Immuni e CovidApp.

I meccanismi e gli standard tecnici dichiarati, sono risultati coerenti con gli obiettivi di sfruttare le possibilità e le caratteristiche della tecnologia digitale per massimizzare la

velocità e la capacità in tempo reale di risposta alla pandemia. Inoltre, essi sono risultati aderenti al modello europeo e orientati al pieno rispetto delle leggi e dei principi europei in materia di privacy e di protezione dei dati personali. In particolare, queste due soluzioni tecnologiche ritenute, in base all'analisi svolta dal gruppo di lavoro, migliori per poter avanzare ad una fase di test sul campo da svolgersi in parallelo su entrambe, sembrano essere tecnologie affidabili e adeguate per il tracciamento della prossimità, per una sicura anonimizzazione dei dati, per creare un contatto tra l'utilizzatore della tecnologia e le figure sanitarie di riferimento, per interagire con interfacce di scambio di dati digitali (API).

Occorre rilevare che per entrambe le soluzioni Immuni e CovidApp sarà necessario svolgere delle attività di personalizzazione e adattamento per renderle compatibili con gli scenari operativi che verranno definiti. La soluzione Immuni utilizza la tecnologia sviluppata dal Consorzio Progetto Europeo PEPP-PT, promettendo quindi maggiori garanzie di interoperabilità e anonimizzazione dei dati personali. Tale soluzione inoltre risulta essere ad uno stadio di sviluppo più avanzato della soluzione CovidApp.

Al fine di poter adottare la soluzione tecnologica più efficace per il *contact tracing* quale componente importante dell'insieme di misure che devono essere messe in campo per la gestione della situazione emergenziale e post-emergenziale, riveste particolare importanza un processo attento ancorché veloce di validazione e messa in esercizio della soluzione tecnologica prescelta, che garantisca il raggiungimento degli obiettivi previsti. Per questa ragione, è opportuno che il processo di implementazione preveda il test in parallelo delle due soluzioni tecnologiche individuate: Immuni, come soluzione che appare all'esito di questa prima valutazione più adeguata e CovidApp, come una buona soluzione alternativa e/o di riserva.

Questo approccio prudenziale serve infatti per avere la garanzia di poter disporre di almeno una soluzione da mettere in campo, anche quando si verificasse, in una sperimentazione concreta, il fallimento per qualunque motivo della funzionalità e/o dei livelli prestazionali richiesti dell'altra opzione alternativa. La fase di test include ovviamente sia la verifica della sicurezza sull'intero codice sorgente (a cura del comparto di *intelligence*) sia la verifica del funzionamento in campo da svolgersi in diverse aree circoscritte del territorio. Si tratterà in ogni caso, indipendentemente dalla soluzione tecnologica che anche ai test di verifica dovesse risultare preferita e più affidabile, di un processo dinamico in evoluzione migliorativa che da una prima versione tecnologica passerà a versioni più avanzate e performanti dal punto di vista sia tecnico che di utilizzo concreto. Pertanto, grande importanza assume a questo riguardo una pianificazione di sviluppo agile che preveda una serie di rilasci scaglionati nel tempo dell'utilizzo della tecnologia.

La proposizione della soluzione tecnologica per il *contact-tracing* che uscirà vincente ai test, prima di essere implementata sul campo, dovrebbe infine essere calata in un quadro strategico-organizzativo più ampio a carico del decisore politico, il quale, per controllare la trasmissione dei contagi, dovrebbe tenere in considerazione non solo altre misure di prevenzione (ad esempio il distanziamento sociale per fasce di popolazione particolarmente fragili) in aggiunta a quelle basate su soluzioni tecnologiche per il *contact tracing* ma anche strategie di azione di carattere generale. Tale strategia permette una efficiente applicazione delle azioni preventive anche verso alcuni segmenti della popolazione Italiana ad alto rischio come gli anziani e il personale sanitario. Negli scenari studiati, è evidente che l'uso di tecnologie per il contact tracing ha la maggiore efficacia prima del termine del periodo di lockdown, quando le misure di isolamento hanno consentito di ridurre il più possibile il tasso di riproduzione di base dell'infezione.

Decisioni richieste alle autorità pubbliche

Decisioni richieste alle autorità pubbliche

Per mettere in esercizio il sistema di *contact tracing*, il decisore pubblico dovrebbe:

A. **Nominare un Program Manager** con piena delega decisionale sul progetto da parte dell'autorità pubblica, al fine di garantire presidio e tempestività nell'implementazione e nel governo dei processi tecnologici.
B. **Scegliere tra le principali opzioni tecnico-organizzative** che impattano su questioni chiave di salute pubblica e di tutela della privacy. Si sollecita quindi una decisione immediata ed esplicita su ciascuno dei seguenti punti:

    1. *Policy per le tecnologie di contact tracing.* I sistemi di *tracing* e le proposte selezionate possono avvalersi di strumenti di rilevazione dei contatti che hanno diversi livelli di impatto atteso sull'efficacia degli interventi di salute pubblica e sul trattamento dei dati personali. Le opzioni proposte sono:
        a) **Solo tecnologie di prossimità senza geolocalizzazione (Bluetooth-LE)** come da modello europeo proposto da PEPP-PT (Pan-European Privacy Preserving Proximity Tracing). Vantaggi: migliore protezione dei dati grazie a codici identificativi univoci che contraddistinguono le installazioni delle applicazioni, resi sufficientemente anonimi, in aderenza al modello PEPP-PT. Svantaggi: minore copertura di situazioni con bassa presenza di device abilitati, mancata indicazione di luoghi di possibile contaminazione ambientale da sanitizzare.

b) **Bluetooth-LE + GPS e/o altre tecnologie che consentano la geolocalizzazione** (solo dei singoli punti di potenziale contagio, non dei percorsi personali, con criptazione dei dati e dietro *opt-in* informato). Vantaggi: maggiore copertura rispetto alla base di smartphone diffusi in Italia ed Europa, maggiore potenziale per l'identificazione di luoghi da sanitizzare. Svantaggi: uso di informazioni riconducibili a dati di carattere personale (posizione del *device*).

2. *Policy da applicare per allertamento a seguito di contagio*. Nel caso in cui un cittadino dotato di app risultasse positivo ai test, è possibile attivare due diverse procedure di allertamento:
   a. **Procedura manuale e volontaria:** (come da modello PEPP-PT) questa opzione prevede un'autorizzazione esplicita e un'azione tecnica da parte del cittadino (foto di un codice QR o immissione di un codice rilasciato dall'autorità sanitaria in caso di test positivo al virus) affinché la propria storia dei contatti anonimizzati venga trasmessa ai server delle autorità e quindi consenta di avviare il processo di allertamento. Vantaggi: i dati sui contatti risiedono solo sul *device* del soggetto. Svantaggi: maggior rischio di malfunzionamenti nella procedura di invio dati, nonché di mancato adempimento spontaneo e/o di ritardo temporale nell'adempimento da parte del cittadino, con l'effetto di ridurre l'efficacia del *contact tracing*.
   b. **Procedura pre-autorizzata automatica:** la seconda opzione prevede che la lista dei contatti anonimizzati sia a disposizione dell'autorità sanitaria, con pre-autorizzazione concessa dal cittadino al momento dell'installazione della app; Vantaggi: massima tempestività ed efficacia del processo di allertamento dei contatti. Svantaggi: i dati dei contatti risiedono sui server dell'autorità pubblica, con i rischi caratteristici della centralizzazione di una base dati, mitigabili con opportune soluzioni tecnologiche.
3. *Policy da applicare per garantire l'enforcement delle azioni di carattere sanitario conseguenti*. A seguito della rilevazione di un caso positivo e dell'allertamento dei soggetti con cui è entrato in contatto, devono seguire azioni di carattere sanitario (ad esempio la quarantena e/o l'autoisolamento per i soggetti entrati in contatto con il caso positivo), che possono essere intraprese in base alle seguenti opzioni:
   a. **Procedura volontaria**: questa opzione prevede che i contatti esposti al rischio di contagio rimangano non identificati (quindi non conosciuti alle autorità sanitarie) e che pertanto essi si assoggettino spontaneamente ai provvedimenti di contenimento indicati nel

messaggio di allertamento inviato al loro *device*. Vantaggi: maggior protezione dei dati personali, anche dopo un possibile allertamento sul rischio di contagio. Svantaggi: maggiori rischi di mancata adesione e/o di ritardo temporale nell'adesione alle misure di contenimento da parte del contatto allertato, con l'effetto di ridurre l'efficacia del *contact tracing*.

b. **Procedura proattiva**: questa opzione prevede (come da corrente prassi di *contact tracing* manuale su linee guida OMS/ECDC) che l'autorità sanitaria richieda e ottenga l'identificazione nominale da parte dei soggetti destinatari dei messaggi di allertamento a seguito di avvenuto contatto con pazienti positivi, prevedendo opportune sanzioni per le eventuali inadempienze. Vantaggi: massima tempestività ed efficacia delle azioni di contenimento dei contatti esposti a potenziale trasmissione del contagio, migliore *compliance* attesa. Svantaggi: raccolta di dati dell'app, a priori ed indipendentemente dal processo di *contact tracing*, necessità di opportuna comunicazione e coinvolgimento dei cittadini.

Bibliografia

1. Abbott S, Hellewell J, Munday J et al., *Temporal variation in transmission during the COVID-19 outbreak*. Centre for Mathematical Modelling of Infectious Disease, 2020, https://cmmid.github.io/topics/covid19/current-patterns-transmission/global-time-varying-transmission.html

2. Ferretti L, Wymant C, Kendall M et al, *Quantifying dynamics of SARS-CoV-2 transmission suggests that epidemic control and avoidance is feasible through instantaneous digital contact tracing,* 2020, doi:https://doi.org/10.1101/2020.03.08.20032946, available at: https://bdi-pathogens.shinyapps.io/covid-19-transmission-routes/

3. McLean E, Pebody RG, Campbell C, Chamberland M, Hawkins C, Nguyen-Van-Tam JS, Oliver I, Smith GE, Ihekweazu C, Bracebridge S, Maguire H, Harris R, Kafatos G, White PJ, Wynne-Evans E, Green J, Myers R, Underwood A, Dallman T, Wreghitt T, Zambon M, Ellis J, Phin N, Smyth B, McMenamin J, Watson JM. *Pandemic (H1N1) 2009 influenza in the UK: clinical and epidemiological findings from the first few hundred (FF100) cases*. Epidemiol Infect. 2010;138:1531-41

4. Crook P, Smith-Palmer A, Maguire H, McCarthy N, Kirkbride H, Court B, Kanagarajah S, Turbitt D, Ahmed S, Cosford P, Oliver I. *Lack of Secondary Transmission of Ebola Virus from Healthcare Worker to 238 Contacts*, United Kingdom, December 2014. Emerg Infect Dis. 2017;23:2081-2084

5. Vaughan A, Aarons E, Astbury J, Balasegaram S, Beadsworth M, Beck CR, Chand M, O'Connor C, Dunning J, Ghebrehewet S, Harper N, Howlett-Shipley R, Ihekweazu C, Jacobs M, Kaindama L, Katwa P, Khoo S, Lamb L, Mawdsley S, Morgan D, Palmer R, Phin N, Russell K, Said B, Simpson A, Vivancos R, Wade M, Walsh A, Wilburn J. *Two cases of monkeypox imported to the United Kingdom*, September 2018. Euro Surveill. 2018;23
6. Matt J Keeling et al., *The Efficacy of Contact Tracing for the Containment of the 2019 Novel Coronavirus (COVID-19)*, medRxiv doi: https://doi.org/10.1101/2020.02.14.20023036