“IMMUNI” ALLA PROVA DELLE LINEE GUIDA EDPB 4-2020

Scopo del presente contributo è quello di instaurare una relazione e confrontare le cautele/caratteristiche definite per la 'app' “Immuni” dall'art. 6 (“sistema di allerta Covid-19”) del Decreto Legge n. 28 del 30 aprile 2020 con i principali requisiti definiti dall'European Data Protection Board (Comitato europeo per la protezione dei dati) nelle recenti Linee Guida n. 4/2020 (l'adozione è del 21 aprile scorso) sull'uso dei dati di localizzazione e degli strumenti per il tracciamento dei contatti nel contesto dell’emergenza legata al Covid-19.

Il raffronto dovrebbe permettere di rispondere alla domanda: **“Immuni” è coerente con l'impianto della normativa di protezione dei dati personali (o quanto meno con le dette Linee Guida), oppure ci sono degli elementi di contrasto e/o di incerta compatibilità che meritano di essere considerati e soppesati**?

Il presupposto giuridico fondamentale di questo esercizio è che le norme sulla protezione dei dati personali - e, in particolare, proprio quelle a garanzia della 'privacy' dei cittadini che si preoccupano, in soldoni, di portare/mantenere le loro persone/vite al riparo da occhi/sguardi indiscreti - **non possano e non debbano essere derogate**, neppure in una situazione come quella generata dalla odierna pandemia.

In un certo senso, è come se la pandemia da Covid-19 finisse per costituire un involontario, gigantesco **'stress-test' per il Governo italiano e per le istituzioni pubbliche interessate**, in grado di rivelare al cittadino **quanta e quale riserva di cultura garantista** – e, più specificamente, 'privacysta' - **esse siano capaci di esprimere**.

Il raffronto è eseguito avvalendosi di una tabella - in calce a questa introduzione - composta di n. 2 colonne: in quella sinistra sono articolati, in successione, i punti delle Linee Guida (ritenuti) rilevanti per il caso specifico; nella colonna destra sono riportati i periodi o commi dell'art. 6 del D.L. 28/2020 e/o considerazioni/appunti circa il suo contenuto, in quanto correlati/correlabili ai contenuti delle Linee Guida a fianco.

Inutile dire come questo sia da considerare un '**work in progress**', aperto a contributi e ad appunti anche dissonanti.

Prima di entrare nel vivo del raffronto mi permetto, tuttavia, una domanda/osservazione di carattere, per così dire, sistemico (ormai del tutto accademica, ovvero utile ad una riflessione critica individuale, sì, ma del tutto inservibile nella situazione che ci tocca, in cui le decisioni fondamentali sono già state prese, addirittura prima dell'avvento del decreto legge): **se la scelta è caduta sul modello di una (unica) 'app' pubblica, si è sicuri che sia questo il modello più adeguato?**

Alcuni osservatori hanno sostenuto che una 'app' del genere avrebbe dovuto essere predisposta già nella fase iniziale del contagio e, in ogni caso, la decisione assunta pare rispondere ad un criterio di necessità ed urgenza (infatti - si dovrebbe dire – la disposizione correlata è situata all'interno di un decreto legge...). Tutto questo non annulla il convincimento che, anche se si fosse eseguita una seria programmazione - ad ampio raggio e tempestiva, come dovrebbe essere -, sarebbe comunque stata scartata a priori la possibilità di dare vita ad un **sistema plurale**, con la **progettazione e lo sviluppo di più**

'app' in concorrenza tra loro, pur entro una cornice di regole/misure di sicurezza valevoli per tutti i soggetti/titolari in esso impegnati.
Sul punto proprio le Linee Guida non solo non vincolano (né potrebbero, d'altronde) gli interpreti e gli attuatori ad un preciso assetto, ma non sembrano neppure escludere la possibilità di un modello realmente alternativo, se è vero che nella introduzione, al punto 1, si premette che "Governi e soggetti privati si stanno orientando verso l'uso di soluzioni basate sui dati nell'ambito della risposta alla pandemia causata dal Covid-19, e ciò suscita numerose preoccupazioni in materia di tutela della vita privata". D'altronde, sia che si dovesse/debba trattare di soggetti pubblici che di privati, invariabilmente **i dati e le tecnologie utilizzati per contribuire alla lotta al Covid-19 debbono/dovranno servire** (punto 4) **"a dare maggiori strumenti alle persone, piuttosto che a controllarle, stigmatizzarle o reprimerne i comportamenti"**; mentre nel capitolo 3, al punto 25 (dedicato proprio alla 'app' per il tracciamento dei contatti), se da un lato il Comitato indica l'ipotesi di un sistema in cui la titolarità del trattamento sia assunta dalle autorità sanitarie nazionali, dall'altro afferma nel prosieguo che **"**si possono comunque prendere in considerazione altre configurazioni di titolarità", senza fornire ulteriori specificazioni.
Insomma, **l'attenzione e la preoccupazione del Comitato non potevano appuntarsi sul "chi", bensì sul "come"**; cioè sulle condizionalità, sul rispetto rigoroso di principi e sulla applicazione di misure concretamente orientate a garantire il rispetto dei diritti individuali, a prescindere dalla natura e dal numero dei possibili titolari dei trattamenti. Perché, come conclude il Comitato (cfr. punto 49), "**a nessuno dovrebbe essere chiesto di scegliere tra una risposta efficace all'attuale crisi e la tutela dei diritti fondamentali**".
Paolo Marini

Tabella di raffronto

LINEE GUIDA	ART. 6 D.L. 28/2020 con annotazioni / considerazioni
1. Introduzione e contesto	
1. **Governi e soggetti privati** si stanno orientando verso l'uso di soluzioni basate sui dati nell'ambito della risposta alla pandemia causata dal COVID-19, e ciò suscita numerose **preoccupazioni in materia di tutela della vita privata**.	
2. Il Comitato europeo per la protezione dei dati sottolinea che il quadro giuridico in materia di protezione dei dati è stato concepito per essere flessibile e, in quanto tale, è in grado di conseguire una risposta efficace per limitare la pandemia e **proteggere i diritti umani e le libertà fondamentali**.	**Le norme a protezione dei diritti umani e delle libertà fondamentali, in quanto riconducibili ai Trattati UE e alla stessa Costituzione, sono nella gerarchia delle fonti del diritto al di sopra degli atti aventi forza di legge ordinaria.** **E' per ciò irrilevante che l'art. 6 non contenga un richiamo a quelle norme.**
3. Il Comitato è fermamente convinto che, ove sia necessario ricorrere al trattamento di dati personali per gestire la pandemia causata dal	**L'inciso** "ove sia necessario ricorrere al trattamento di dati personali per gestire la pandemia (...)"**, più che suggerire che una**

COVID-19, **la protezione dei dati è indispensabile per generare un clima di fiducia, creare le condizioni per l'accettabilità sociale di qualsiasi soluzione e garantire, pertanto, l'efficacia di tali misure**. Poiché il virus non conosce confini, appare preferibile sviluppare un approccio comune europeo in risposta alla crisi attuale, o almeno realizzare una cornice di interoperabilità.	**soluzione di contrasto al virus potrebbe/dovrebbe non comportare alcun trattamento di dati personali, allude più realisticamente (come dimostra il prosieguo) alla necessità di procurare ai trattamenti pur strettamente necessari, misure di sicurezza e modalità di informazione al pubblico tali da generare un clima di fiducia.** **Quanto all'approccio comune europeo e alla cornice di interoperabilità, l'art. 6 non contiene alcun cenno o riferimento.**
4. Il Comitato ritiene, in via generale, che **i dati e le tecnologie utilizzati per contribuire alla lotta al COVID-19** debbano servire a **dare maggiori strumenti alle persone, piuttosto che a controllarle, stigmatizzarle o reprimerne i comportamenti**. Inoltre, mentre i dati e le tecnologie possono essere strumenti importanti, essi hanno limiti intrinseci e non possono che far leva sull'efficacia di altre misure di sanità pubblica. I principi generali di efficacia, necessità e proporzionalità devono guidare qualsiasi misura adottata dagli Stati membri o dalle istituzioni dell'UE che comporti il trattamento di dati personali per combattere il COVID-19.	**Il primo periodo contiene un passaggio cruciale delle LG, perché individua un criterio generale la cui conferma nella realtà – premessi la progettazione, lo sviluppo e l'implementazione di qualsivoglia soluzione - non può presumersi, non può essere data per scontata.**
5. Le presenti linee-guida chiariscono le condizioni e i principi per l'uso proporzionato dei dati di localizzazione e degli strumenti di tracciamento dei contatti, in due ambiti specifici : - Utilizzo dei dati di localizzazione a supporto della risposta alla pandemia tramite la definizione di modelli della diffusione del virus, al fine di valutare l'efficacia complessiva di misure di isolamento e quarantena; - **Utilizzo del tracciamento dei contatti per informare le persone che sono probabilmente entrate in contatto ravvicinato con soggetti successivamente confermati positivi, al fine di interrompere tempestivamente la trasmissione del contagio**.	**Per l'art. 6, comma 1, primo periodo, prima parte, il fine della 'app' è** "di allertare le persone che siano entrate in contatto stretto con soggetti risultati positivi e tutelarne la salute attraverso le previste misure di prevenzione nell'ambito delle misure di sanità pubblica legate all'emergenza COVID-19". **La scelta del legislatore è tutta giocata sul secondo ambito, con esclusione del primo, incentrato sull'utilizzo dei dati di localizzazione.**
6. L'efficienza del contributo che le app per il tracciamento dei contatti possono fornire alla gestione della pandemia dipende da molti fattori (ad esempio, percentuale di persone che dovrebbero installarle; **definizione di "contatto" in termini di prossimità e durata**). Inoltre, **tali applicazioni devono far parte di una strategia globale in materia di sanità pubblica per combattere la pandemia**,	**L'art. 6 non contiene alcuna definizione di "contatto" (semmai qualche indizio si può desumere dalla tecnologia Bluetooth adottata da "Immuni"). I riferimenti in esso contenuti sono per lo più a contatto o contatti "stretto/i". Lungi dal pretendere qui (come altrove) che una disposizione di legge debba spingersi a disciplinare elementi di simil dettaglio, è fuor di dubbio che anche una**

compresi, tra l'altro, la sperimentazione e il successivo tracciamento manuale dei contatti ai fini dell'eliminazione di casi dubbi. La loro diffusione dovrebbe essere accompagnata da misure di sostegno volte a garantire che le informazioni fornite agli utenti siano contestualizzate e che le segnalazioni possano essere utili al sistema sanitario pubblico. In caso contrario, queste applicazioni potrebbero non esplicare appieno la propria efficacia.	**definizione di contatto (o di contatto stretto) entri a pieno titolo nel novero delle informazioni da rendere al pubblico preventivamente, affinché sia generato un clima di consapevolezza e, quindi, di fiducia.**
8. (...) il Comitato si è già pronunciato sul fatto che il ricorso alle app per **il tracciamento dei contatti dovrebbe essere volontario e non dovrebbe basarsi sulla tracciabilità dei movimenti individuali**, bensì sulle informazioni di prossimità relative agli utenti.	**Nel primo periodo dell'art. 6, comma 1, si afferma che** "è istituita una piattaforma unica nazionale per la gestione del sistema di allerta dei soggetti che, a tal fine, hanno installato, su base volontaria, un'apposita applicazione sui dispositivi di telefonia mobile". **Il criterio della volontarietà della 'app' è formalmente soddisfatto.**
2. Utilizzo dei dati relativi all'ubicazione	
2.1. Fonti dei dati relativi all'ubicazione	
9. Per la modellizzazione della diffusione del virus e dell'efficacia complessiva delle misure di confinamento, esistono due principali fonti di dati relativi all'ubicazione: • dati relativi all'ubicazione raccolti da fornitori di servizi di comunicazione elettronica (come gli operatori di telecomunicazioni mobili) nel corso della prestazione del loro servizio; e • dati relativi all'ubicazione raccolti da fornitori di servizi della società dell'informazione, la cui funzionalità richiede l'uso di tali dati (ad esempio, navigazione, servizi di trasporto, ecc.).	**Come già visto a proposito del punto 5, per l'art. 6, comma 2, lett. c), parte finale:** "(…) e' esclusa in ogni caso la geolocalizzazione dei singoli utenti". **Non ci sarà dunque trattamento di dati relativi all'ubicazione e l'intero capitolo 2 delle LG potrebbe dunque saltarsi a pie' pari, se non fosse che molte delle considerazioni in esso contenute, nei punti ritenuti più significativi, meritano adeguata lettura.** **Ma, soprattutto, non è da escludere - come si può constatare più oltre – che queste considerazioni si rivelino importanti ai fini della disamina dell'art. 6, comma 3.**
2.2. Utilizzo di dati anonimizzati relativi all'ubicazione	
14. Il Comitato sottolinea che, **per quanto riguarda l'utilizzo dei dati relativi all'ubicazione, occorre sempre privilegiare il trattamento di dati anonimi** piuttosto che di dati personali.	**Le LG non escludono l'utilizzo di dati personali. Si limitano a stabilire un criterio nettamente preferenziale in favore dell'utilizzo di dati non personali, ovvero anonimi. Nel caso di "Immuni" è più che probabile che il trattamento investirà, nel diverso contesto del contact tracing (o recording), dati personali.**
15. **L'anonimizzazione fa riferimento all'uso di una serie di tecniche finalizzate a eliminare la possibilità di collegare i dati a una persona fisica identificata o identificabile con uno sforzo "ragionevole"**. Questo "test di	**Il capitolo 2.2. delle LG è particolarmente interessante in quanto dà conto:** **- della criticità delle procedure di anonimizzazione;** **- della difficoltà specifica di parlare di**

ragionevolezza" deve tenere conto sia degli aspetti oggettivi (tempi, mezzi tecnici) sia di elementi di contesto che possono variare caso per caso (rarità di un fenomeno, la densità di popolazione, la natura e il volume dei dati). Se i dati non superano tale test, non sono anonimizzati e pertanto rientrano nel campo di applicazione del regolamento generale sulla protezione dei dati.	**'anonimizzazione' quando oggetto della procedura siano dati relativi all'ubicazione;** **- della distinzione normativa e fattuale tra 'anonimizzazione' e 'pseudonimizzazione';** **- della necessità di comunicare in modo trasparente la metodologia di anonimizzazione eventualmente utilizzata.**
17. **Il concetto di anonimizzazione tende ad essere frainteso e spesso confuso con la pseudonimizzazione**. **Mentre l'anonimizzazione consente di utilizzare i dati senza restrizioni, i dati pseudonimizzati rientrano nel campo di applicazione del regolamento generale sulla protezione dei dati**.	
18. Esistono molte opzioni per conseguire un'anonimizzazione efficace, ma con un caveat. I dati non possono essere resi anonimi isolatamente, il che significa che solo intere serie o interi insiemi di dati sono passibili di anonimizzazione. In tal senso, **qualsiasi intervento su un dato isolato o sulla serie storica di dati riferibili a un singolo interessato (mediante cifratura o altre trasformazioni matematiche) può essere considerato, nel migliore dei casi, una pseudonimizzazione**.	
19. I processi di anonimizzazione e i tentativi di re-identificazione sono oggetto di numerosi studi e ricerche. È fondamentale che ogni titolare che implementi soluzioni di anonimizzazione si mantenga aggiornato sugli sviluppi recenti in questo campo, in particolare per quanto riguarda i **dati relativi all'ubicazione** (provenienti da operatori delle telecomunicazioni e/o da servizi della società dell'informazione) che sono **notoriamente difficili da anonimizzare**.	
20. In effetti, un ampio corpus di ricerche ha dimostrato che **dati relativi all'ubicazione ritenuti anonimi possono di fatto non esserlo**. **Le tracce di mobilità dei singoli individui sono caratterizzate intrinsecamente da forte correlazione e univocità**. Pertanto, in determinate circostanze possono essere vulnerabili ai tentativi di re-identificazione.	
23. Infine, data la complessità dei processi di anonimizzazione, si raccomanda con forza di **garantire la trasparenza per quanto riguarda**	

la metodologia di anonimizzazione utilizzata.	
3. App per il tracciamento dei contatti	
3.1. Analisi giuridica generale	
24. Il **monitoraggio sistematico e su larga scala dell'ubicazione e/o dei contatti tra persone fisiche** costituisce una **grave interferenza nella vita privata**. Essa può essere **legittimata** solo facendo affidamento su un'**adozione volontaria** da parte degli utenti per ciascuno dei rispettivi scopi. Ciò implica, in particolare, che le persone che non intendono o non possono utilizzare tali applicazioni non dovrebbero subire alcun pregiudizio.	**Già segnalata (in corrispondenza del punto 8) la volontarietà della adozione della 'app', è quindi stabilito dall'art. 6, comma 4, che** "il mancato utilizzo dell'applicazione di cui al comma 1 non comporta alcuna conseguenza pregiudizievole ed è assicurato il rispetto del principio di parità di trattamento"**.**
25. Per garantire il rispetto del principio di responsabilizzazione, dovrebbe essere **definita chiaramente la titolarità del trattamento** di un'eventuale app per il tracciamento di contatti. Il Comitato ritiene che le autorità sanitarie nazionali possano essere i titolari di tale trattamento; si possono comunque prendere in considerazione altre configurazioni di titolarità. In ogni caso, se il processo di diffusione delle app per il tracciamento dei contatti coinvolge diversi attori, devono essere definiti con chiarezza e fin dall'inizio i ruoli e le responsabilità rispettive e di tutto ciò devono essere informati gli utenti.	**In base all'art. 6, comma 1 (dal secondo periodo in poi, premessa l'istituzione di una piattaforma unica nazionale per la gestione del sistema di allerta),** "il Ministero della salute, in qualità di titolare del trattamento, si coordina, sentito il Ministro per gli affari regionali e le autonomie, anche ai sensi dell'articolo 28 del Regolamento (UE) 2016/679, con i soggetti operanti nel Servizio nazionale della protezione civile, di cui agli articoli 4 e 13 del decreto legislativo 2 gennaio 2018, n. 1, e con i soggetti attuatori di cui all'articolo 1 dell'ordinanza del Capo del Dipartimento della protezione civile n. 630 del 3 febbraio 2020, nonché con l'Istituto superiore di sanità e, anche per il tramite del Sistema Tessera Sanitaria, con le strutture pubbliche e private accreditate che operano nell'ambito del Servizio sanitario nazionale, nel rispetto delle relative competenze istituzionali in materia sanitaria connessa all'emergenza epidemiologica da COVID 19, per gli ulteriori adempimenti necessari alla gestione del sistema di allerta e per l'adozione di correlate misure di sanità pubblica e di cura. Le modalità operative del sistema di allerta tramite la piattaforma informatica di cui al presente comma sono complementari alle ordinarie modalità in uso nell'ambito del Servizio sanitario nazionale. Il Ministro della salute e il Ministro per gli affari regionali e le autonomie informano periodicamente la Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e di Bolzano sullo stato di avanzamento del progetto". **Dunque, se al Ministero della salute compete per legge la qualifica di titolare del trattamento, dovrà quindi seguire il**

	necessario inquadramento di tutti i soggetti a vario titolo implicati nel progetto. Se l'espressione "si coordina" farebbe pensare alla contitolarità nei trattamenti ex art. 26, l'espressione "anche ai sensi dell'art. 28 del Regolamento UE 2016/679"**, lascia spazio a tutte le ipotesi di inquadramento coerenti con il regime effettivo dei rapporti.** **E' evidente che, comunque sia affrontato e definito l'argomento, le informazioni da rendere al pubblico dovranno spiegare con chiarezza chi siano gli attori coinvolti e quali siano i rispettivi ruoli e responsabilità.** **Quanto all'art. 6, comma 5, (**"La piattaforma di cui al comma 1 è di titolarità pubblica ed è realizzata dal Commissario di cui all'articolo 122 del decreto-legge 17 marzo 2020, n. 18, convertito, con modificazioni, dalla legge 24 aprile 2020, n. 27, 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. I programmi informatici di titolarità pubblica sviluppati per la realizzazione della piattaforma e l'utilizzo dell'applicazione di cui al medesimo comma 1 sono resi disponibili e rilasciati sotto licenza aperta ai sensi dell'articolo 69 del decreto legislativo 7 marzo 2005, n. 82."**), esso concerne la titolarità (sicuramente in senso tradizionale) della piattaforma nazionale unica: essa compete al Commissario straordinario per l'attuazione e il coordinamento delle misure di contenimento e contrasto dell'emergenza epidemiologica Covid-19. Lo stesso organo/funzione che con ordinanza del 16 aprile 2020 ha individuato/scelto la 'app' "Immuni".**
26. Inoltre, per quanto riguarda il **principio della limitazione delle finalità**, le finalità devono essere sufficientemente specifiche così da escludere trattamenti ulteriori per scopi non correlati alla gestione della crisi sanitaria causata da COVID-19 (ad esempio, per fini commerciali o per le attività di contrasto di matrice giudiziaria o di polizia). Una volta definita con chiarezza la finalità, sarà necessario garantire che l'uso dei dati personali sia adeguato, necessario e proporzionato.	**La finalità (del trattamento) è strettamente correlata al fine stesso della 'app', ex art. 6, comma 1, primo periodo:** "allertare le persone che siano entrate in contatto stretto con soggetti risultati positivi e tutelarne la salute attraverso le previste misure di prevenzione nell'ambito delle misure di sanità pubblica legate all'emergenza". **Sembrano escluse finalità diverse, in base al successivo comma 3, ma con un'eccezione di non poco conto:** "I dati raccolti attraverso l'applicazione di cui al comma 1 non possono

	essere trattati per finalità diverse da quella di cui al medesimo comma 1, salva la possibilità di utilizzo in forma aggregata o comunque anonima, per soli fini di sanità pubblica, profilassi, statistici o di ricerca scientifica, ai sensi degli articoli 5, paragrafo 1, lettera a) e 9, paragrafo 2, lettere i) e j), del Regolamento (UE) 2016/679." **Riportandoci a quanto scritto in corrispondenza del punto 15, va segnalato che:** **- utilizzo in forma aggregata e utilizzo in forma anonima non significano la stessa cosa e comunque l'impegno del legislatore è inequivocamente formalizzato nel senso della anonimizzazione (**"o comunque anonimi"**);** **- tra le informazioni da rendere non potrà mancare l'indicazione della metodologia di anonimizzazione prescelta per tutti i dati (in tal caso la declaratoria delle finalità ulteriori potrebbe essere opportuna ma non sarebbe obbligatoria. Se, infatti, il trattamento dovrà concernere dati anonimi, esso non sarà più soggetto al campo di applicazione del Regolamento UE 2016/679).**
27. Nel contesto di un'app per il tracciamento dei contatti, occorre prestare particolare attenzione al **principio di minimizzazione** e ai **principi della protezione dei dati fin dalla progettazione e per impostazione predefinita** (data protection by design and by default): • **le app per il tracciamento dei contatti non necessitano del tracciamento della posizione dei singoli utenti**. Occorre invece utilizzare i dati di prossimità; • **poiché le app per il tracciamento dei contatti possono funzionare senza l'identificazione diretta delle persone, dovrebbero essere adottate misure adeguate per prevenire la reidentificazione**; • **le informazioni raccolte dovrebbero risiedere nell'apparecchiatura terminale dell'utente** e dovrebbero essere raccolte solo le informazioni pertinenti e solo ove strettamente necessarie.	**Rispetto a questo punto si propongono le seguenti osservazioni:** **L'art. 6, comma 2, lett. b) fa riferimento per impostazione predefinita (art. 25) ai (soli) dati personali "**raccolti dall'applicazione di cui al comma 1 (...) necessari ad avvisare gli utenti dell'applicazione di rientrare tra i contatti stretti di altri utenti accertati positivi al COVID-19, (...), nonché ad agevolare l'eventuale adozione di misure di assistenza sanitaria in favore degli stessi soggetti". **Sempre all'art. 6, comma 2, stavolta però alla lett. c), è definito un criterio coerente con le LG nella misura in cui il trattamento effettuato per allertare i contatti sarà basato** "sul trattamento di dati di prossimità dei dispositivi"**, essendo però esclusa la geolocalizzazione degli utenti/interessati**. **Quanto alla questione di prevenire la reidentificazione, l'art. 6, comma 2, lett. d) fa riferimento alla garanzia su base permanente di** "misure adeguate ad evitare il rischio di reidentificazione degli interessati cui si riferiscono i dati pseudonimizzati oggetto di trattamento"**. Non può sfuggire, tuttavia, che se il trattamento riguarderà dati**

	pseudonimizzati, la reidentificazione si potrà presto o tardi rendere possibile. Allora sarà fondamentale prima stabilire e poi comunicare (agli utenti) chi, quando, come e perché potrà - nella misura in cui ciò sia necessario - avere accesso ai dati. **Quanto alla residenza delle informazioni raccolte - sempre se pertinenti e necessarie - nel device dell'utente, l'art. 6, comma 2, lett. e) si pone in contrasto con tale criterio nel momento in cui vi è stabilito che** "i dati relativi ai contatti stretti siano conservati, anche **(anche, ovvero non solo - ndr)** nei dispositivi mobili degli utenti, per il periodo strettamente necessario al trattamento...". **Dalla lettura complessiva dell'art. 6 non pare in ogni caso di poter desumere che la raccolta dei dati sia limitata come da indicazioni delle LG.**
28. Per quanto riguarda la liceità del trattamento, il Comitato rileva che le app per il tracciamento dei contatti comportano la memorizzazione e/o l'accesso a informazioni già archiviate nell'apparecchiatura terminale dell'utente, che sono soggette all'articolo 5 (3) della direttiva ePrivacy. Se tali operazioni sono strettamente necessarie per consentire al fornitore dell'app di rendere il servizio esplicitamente richiesto dall'utente, il trattamento non richiede il consenso di quest'ultimo. Per le operazioni che non sono strettamente necessarie, il fornitore dovrebbe richiedere il consenso dell'utente.	**Dalla lettura dell'art. 6 si evince, come già osservato, la finalità del trattamento connessa ad "Immuni" ma la disposizione non si occupa di base giuridica del trattamento.** **Anche con riferimento ai successivi punti 29-30, è da notare che la definizione della base giuridica non è pregiudicata dalla volontarietà della 'app'; e che il tenore complessivo dell'art. 6, che non contiene alcun riferimento a meccanismi di rilascio del consenso (trattandosi comunque, va detto, di circostanza non decisiva), fa supporre che la base giuridica potrebbe essere identificata proprio nell'art. 6.1, lett. e).**
29. Inoltre, il Comitato osserva come **la circostanza per cui l'uso di app per il tracciamento dei contatti avvenga su base volontaria non implichi che il trattamento dei dati personali debba necessariamente basarsi sul consenso**. Qualora autorità pubbliche forniscano un servizio sulla base di un mandato conferito dalla legge e conformemente ai requisiti stabiliti da tale legge, la base giuridica più pertinente risulta essere la necessità del trattamento per lo svolgimento di un compito di interesse pubblico, ossia l'articolo 6, paragrafo 1, lettera e), del Regolamento generale sulla protezione dei dati.	
30. L'articolo 6, paragrafo 3, del Regolamento precisa che la base su cui si fonda il trattamento di cui all'articolo 6, paragrafo i), lettera e) è stabilita dal diritto dell'Unione o dello Stato	

membro cui è soggetto il titolare. La finalità del trattamento è definita in tale base giuridica o, per quanto riguarda il trattamento di cui al paragrafo 1, lettera e), è necessaria per l'esecuzione di un compito svolto nel pubblico interesse o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.	
31. Tuttavia, la base giuridica o la misura legislativa che costituisce il fondamento di liceità per l'uso dell'app di tracciamento dei contatti dovrebbero prevedere garanzie significative, compreso un riferimento alla natura volontaria dell'app. Dovrebbe essere inclusa una chiara specificazione delle finalità e delle limitazioni riguardanti l'ulteriore utilizzo dei dati personali, nonché una chiara identificazione del titolare o dei titolari coinvolti. Occorre inoltre individuare le categorie di dati e i soggetti ai quali i dati personali possono essere comunicati, e per quali scopi. A seconda del grado di interferenza, occorre integrare salvaguardie ulteriori tenendo conto della natura, della portata e delle finalità del trattamento. Infine, il Comitato raccomanda di prevedere, non appena possibile, i criteri per stabilire quando l'app dovrà essere disinstallata e a chi spetti assumere tale determinazione.	**L'art. 6, comma 2, lett. a), prescrive che** "gli utenti ricevano, prima dell'attivazione dell'applicazione, ai sensi degli articoli 13 e 14 del Regolamento (UE) 2016/679, informazioni chiare e trasparenti al fine di raggiungere una piena consapevolezza, in particolare, sulle finalità e sulle operazioni di trattamento, sulle tecniche di pseudonimizzazione utilizzate e sui tempi di conservazione dei dati". **Quanto all'art. 6, comma 2, lett. f), per esso** i **diritti degli interessati di cui agli articoli da 15 a 22 del Regolamento (UE) 2016/679 potranno essere esercitati anche con modalità semplificate.** **Possibili osservazioni con riferimento al punto 31 sono già disseminate nei precedenti riquadri. Qui è opportuno sottolineare che:** **- le informative dovranno individuare le categorie di dati e i soggetti ai quali i dati personali possano essere comunicati;** **- debbano essere definiti e comunicati agli utenti i criteri per stabilire quando la 'app' debba essere disinstallata e a chi spetti assumere tale determinazione.** **Si fa sommessamente notare che qui le LG entrano un po' in contraddizione... con se stesse: se e nella misura in cui la 'app' è volontaria, la determinazione circa la sua disinstallazione dovrebbe/dovrà essere prerogativa di ciascun utente. Così anche per "Immuni".**
33. Inoltre, il ricorso a un'app per combattere la pandemia da COVID-19 potrebbe portare alla raccolta di dati relativi alla salute (ad esempio lo status di persona infetta). Il trattamento di tali dati è consentito quando è necessario per motivi di interesse pubblico nel settore della sanità pubblica, nel rispetto delle condizioni di cui all'articolo 9, paragrafo 2, lettera i), del Regolamento, o per le finalità dell'assistenza sanitaria di cui all'articolo 9, paragrafo 2, lettera h), del Regolamento stesso. A seconda della base giuridica individuata, il trattamento in questione potrebbe anche fondarsi sul consenso esplicito	**In continuità con quanto osservato a lato del precedente punto 28, qui si segnala senz'altro la necessità di un completamento della definizione della base giuridica - beninteso se e nella misura in cui debbano divenire oggetto di trattamento anche dati relativi alla salute degli interessati.**

dell'interessato (articolo 9, paragrafo (2), lettera a), del Regolamento).	
34. Conformemente allo scopo iniziale, l'articolo 9, paragrafo 2, lettera j), del Regolamento consente inoltre che i dati relativi alla salute siano trattati ove necessario a fini di ricerca scientifica o a fini statistici.	**Vedansi con riferimento all'art. 6, comma 3, le precedenti osservazioni a fianco del punto 26.**
35. L'attuale crisi sanitaria non dovrebbe trasformarsi in un'occasione per derogare rispetto al principio di limitazione della conservazione dei dati. La conservazione dovrebbe essere limitata alla luce delle reali esigenze e della rilevanza medica (anche con riguardo a considerazioni di natura epidemiologica quali il periodo di incubazione, ecc.) e i dati personali dovrebbero essere conservati solo per la durata della crisi dovuta al COVID-19. Successivamente, di norma, tutti i dati personali dovrebbero essere cancellati o resi anonimi.	**Si riporta l'art. 6, comma 6, per il quale** "l'utilizzo dell'applicazione e della piattaforma, nonché ogni trattamento di dati personali effettuato ai sensi al presente articolo sono interrotti alla data di cessazione dello stato di emergenza disposto con delibera del Consiglio dei ministri del 31 gennaio 2020, e comunque non oltre il 31 dicembre 2020, ed entro la medesima data tutti i dati personali trattati devono essere cancellati o resi definitivamente anonimi." **Ciò che perplime in questo comma è quel "resi definitivamente anonimi", perché un dato reso 'provvisoriamente anonimo' non è anonimo. Emerge, cioè, una qualche confusione mentale del legislatore sull'argomento. La procedura di anonimizzazione è irreversibile e dunque sempre, ex se, "definitiva".** **Quanto all'art. 6, comma 2, lett. e), esso prescrive che** "i dati relativi ai contatti stretti siano conservati, anche nei dispositivi mobili degli utenti, per il periodo strettamente necessario al trattamento, la cui durata è stabilita dal Ministero della salute e specificata nell'ambito delle misure di cui al presente comma; i dati sono cancellati in modo automatico alla scadenza del termine".
36. **Il Comitato ritiene che tali app non possano sostituire, ma solo supportare, il tracciamento manuale dei contatti effettuato da personale sanitario pubblico qualificato, che potrà stabilire con quale probabilità contatti ravvicinati diano luogo a una trasmissione del virus o meno** (ad esempio, in caso di interazioni con una persona protetta da un adeguato equipaggiamento, come può avvenire ad esempio per un addetto alla cassa di un supermercato ecc.). Il Comitato sottolinea che **tutte le procedure e i processi, compresi gli algoritmi implementati dalle app per il tracciamento dei contatti, dovrebbero svolgersi sotto la stretta sorveglianza di personale qualificato al fine di limitare il verificarsi di falsi positivi e negativi**. In	**Il punto 36 è importante, perché indica la necessaria esclusione di processi interamente automatizzati: tutte le procedure e i processi, compresi gli algoritmi implementati dalle 'app' per il tracciamento dei contatti, dovrebbero svolgersi sotto la stretta sorveglianza di personale qualificato, al fine di limitare il verificarsi di falsi positivi e negativi e di ovviare alle conseguenze indesiderabili, al grave impatto sulla vita e sulla libertà degli individui che ne potrebbero derivare.** **L'art. 6 non contiene alcun riferimento alla problematica ma l'accettabilità sociale della 'app' presuppone un sostanziale chiarimento, in sede di comunicazione e di informazioni da rendere al pubblico, su tutte le questioni qui**

particolare, le indicazioni fornite in merito ai passi da compiere successivamente alla ricezione di un alert non dovrebbero basarsi unicamente su un trattamento automatizzato.	**sollevate. Ciò vale anche con riferimento ai punti 37 e 38.**
37. Al fine di garantire la correttezza dei trattamenti, il rispetto del principio di responsabilizzazione e, più in generale, la conformità con la legge, **gli algoritmi devono essere verificabili e devono essere soggetti a un riesame periodico da parte di esperti indipendenti**. Il codice sorgente dovrebbe essere reso pubblico così da assicurare la più ampia trasparenza possibile.	**Nessun riferimento nell'art. 6 a quanto sollevato dal punto 37. L'algoritmo è un ulteriore elemento da aggiungere al corposo capitolo delle informazioni da comunicare al pubblico.**
38. **Vi sarà sempre, in una certa misura, la possibilità del verificarsi di falsi positivi**. Poiché l'identificazione di un rischio di infezione può avere un forte impatto sui singoli individui, ad esempio imponendo l'autoisolamento fino a negativizzazione del test, è indispensabile poter effettuare correzioni dei dati e/o dei risultati delle analisi successive. Naturalmente ciò vale solo in presenza di situazioni o implementazioni in cui il trattamento e la conservazione dei dati sono configurati in modo da permettere tecnicamente di apportare le correzioni suddette, e ove sia probabile il verificarsi degli effetti negativi di cui sopra.	
39. Infine, il Comitato ritiene che debba essere effettuata una **valutazione d'impatto sulla protezione dei dati prima di implementare le app in questione**, in quanto il trattamento configura una probabilità di rischio elevato (dati relativi alla salute, adozione prevista su larga scala, monitoraggio sistematico, uso di una nuova soluzione tecnologica). Il Comitato raccomanda vivamente la **pubblicazione degli esiti di tali valutazioni**.	**In base all'art. 6, comma 2,** "il Ministero della salute, all'esito di una valutazione di impatto, costantemente aggiornata, effettuata ai sensi dell'articolo 35 del Regolamento(UE) 2016/679, adotta misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato ai rischi elevati per i diritti e le libertà degli interessati, sentito il Garante per la protezione dei dati personali ai sensi dell'articolo 36, paragrafo 5, del medesimo Regolamento (UE) 2016/679 e dell'articolo 2-quinquiesdecies del Codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196, (….)." **E' da rammentare che il titolare non è tenuto ad interpellare il Garante quando abbia eseguito la DPIA con esito positivo (assenza di rischio elevato in assenza di misure per attenuare il rischio, cfr. art. 36.1). Non casualmente il comma 2 fa riferimento all'art. 2-quinquiesdecies del Codice privacy, dettato proprio per l'ipotesi di trattamento che presenta rischi elevati per l'esecuzione di un compito di interesse pubblico.**

	Viene da osservare che con la DPIA il titolare dovrebbe 'lanciare', trattare e risolvere non poche tra le questioni sollevate lungo questa trattazione, includendovi anche le misure di prevenzione e gestione dei falsi positivi. **Necessaria al famoso clima di fiducia è anche la pubblicazione degli esiti della DPIA.**
3.2. Raccomandazioni e requisiti funzionali	
40. Conformemente al **principio di minimizzazione**, tra le altre misure in ossequio al principio di protezione dei dati fin dalla progettazione e per impostazione predefinita, i dati trattati dovrebbero essere limitati a quelli strettamente necessari. L'app non dovrebbe raccogliere informazioni non correlate o non necessarie come, per esempio, dati anagrafici, identificativi, di comunicazione, voci di directory del dispositivo, messaggi, registrazioni di chiamate, dati relativi all'ubicazione, identificativi del dispositivo, ecc. .	**Come già visto, l'art. 6, comma 2, lett. b) limita la raccolta dei dati a quelli** "necessari ad avvisare gli utenti dell'applicazione di rientrare tra i contatti stretti di altri utenti accertati positivi al COVID-19, (...), nonché ad agevolare l'eventuale adozione di misure di assistenza sanitaria in favore degli stessi soggetti". **Le raccomandazioni contenute in questo capitolo riguardano, in particolare, aspetti tecnici che l'art. 6 non definisce e che pure debbono essere affrontati e risolti dal titolare, prima dell'avvio ufficiale e dell'utilizzo della 'app'.**
41. I dati trasmessi dall'app devono includere solo **identificatori univoci e pseudonimi, generati dall'app e specifici di tale app**. Tali identificatori devono essere rinnovati regolarmente, secondo una frequenza compatibile con lo scopo di contenere la diffusione del virus e sufficiente a limitare il rischio di identificazione e di localizzazione fisica delle persone.	
42. Le **applicazioni per il tracciamento dei contatti** possono seguire un **approccio centralizzato o decentrato**. Entrambe le opzioni sono praticabili, a condizione che siano in vigore adeguate misure di sicurezza, ed entrambe comportano una serie di vantaggi e svantaggi. Pertanto, la fase di progettazione delle app dovrebbe sempre prevedere un esame approfondito di entrambi gli approcci, ponderandone attentamente gli effetti in termini di protezione dei dati e privacy nonché i possibili impatti sui diritti delle persone.	**L'art. 6 (al comma 2, lett. e) lascia del tutto impregiudicata la questione.**
43. Ogni server coinvolto nel sistema di tracciamento dei contatti deve raccogliere soltanto la **cronologia dei contatti** o gli **identificativi pseudonimizzati di un utente diagnosticato come infetto a seguito di un'adeguata valutazione effettuata dalle autorità sanitarie e di un'azione volontaria**	**Per l'art. 6, comma 2, lett. c)** "(…) il trattamento effettuato per allertare i contatti sia basato sul trattamento di dati di prossimità dei dispositivi, resi anonimi oppure, ove ciò non sia possibile, pseudonimizzati."

dell'utente stesso. Alternativamente, il server deve conservare un elenco degli identificativi pseudonimizzati di utenti infetti o la rispettiva cronologia dei contatti solo per il periodo necessario a informare gli utenti potenzialmente infetti della loro avvenuta esposizione, senza tentare di individuare tali utenti potenzialmente infetti.	
45. Si deve fare ricorso a **tecniche crittografiche di ultima generazione** per garantire la conservazione sicura dei dati memorizzati nei server e nelle app, nonché gli scambi tra le app e il server remoto. Occorre inoltre implementare sistemi di autenticazione reciproca tra l'app e il server.	**Ci si limita ad osservare il carattere fondamentale – se del caso - di questa misura di sicurezza (crittografia), soprattutto pensando a rischi di attacchi informatici.**
46. La segnalazione nell'app di utenti infetti da COVID-19 deve essere soggetta a idonea procedura, ad esempio mediante l'**impiego di un codice monouso correlato a una identità pseudonima della persona infetta e collegato a un laboratorio o a un operatore sanitario**. Se la conferma non può essere ottenuta in modo sicuro, non dovrebbe aversi alcun trattamento di dati sulla base di una presunzione di validità dello status relativo all'utente.	
47. Il titolare del trattamento, in collaborazione con le autorità pubbliche, deve fornire **informazioni chiare e inequivocabili sul link ove scaricare l'app ufficiale** per il tracciamento dei contatti al fine di ridurre il rischio che gli utenti utilizzino un'app di terze parti.	**Il titolare è/sarà una autorità pubblica e certamente dovrà provvedere anche a questa incombenza.**

Avv. Paolo Marini, Foro di Firenze