GIUSTIZIA INSIEME

Diritto dell"emergenza Covid-19 e recovery fund" class="voce">

App Immuni: una storia stran(ier)a e incompiuta di Lara Trucco

di Lara Trucco

25 giugno 2020

***App* Immuni: una storia stran(ier)a e incompiuta**

di Lara Trucco

Sommario: 1. Premessa. – 2. La fase I: la *App* tra Unione europea e Governo italiano. – 3. La fase II: tra i due litiganti…*Google* ed *Apple* godono. – 4. La fase III: …tornando dalla *App* personale di *tracing*. – 5. …per andare alla piattaforma multinazionale di *tracking*. – 6. …passando dal server nazionale di *testing* ed *identification*. – 7. Una "costituente tecnologica" eurounitaria (ed italiana)?

1. *Premessa*

La vicenda della cd. "*App Immuni*" (nel prosieguo: *App*) offre uno spaccato di un certo interesse delle dinamiche in atto sul fronte delle strategie di contrasto al Covid-19 e delle relative criticità: questioni su cui ci si propone di portare in questa sede l'attenzione.

All'indomani dell'ufficializzazione dello stato di pandemia, infatti, l'opportunità di ricorrere all'impiego di sistemi di tracciamento per interrompere la diffusione dei contagi secondari è entrato, com'è noto, a pieno titolo nel dibattito scientifico ed altresì mediatico, portando il nostro Stato, alla pari di altri, ad impegnarsi nella loro adozione.

Le strade seguite sono state varie, essendosi passati da soluzioni tecnologiche più blande e meno efficaci; ad altre, invece, maggiormente intrusive rispetto ai dati personali "sensibili" e "supersensibili", i quali, anche per tale motivo, hanno suscitato maggiore attenzione, rischiando, tra l'altro, di mettere a repentaglio altri diritti fondamentali, o di esporre ad una stigmatizzazione individuale e sociale i soggetti che hanno subito il contagio. Di qui, il complesso tema del bilanciamento dei valori in campo, specie una volta constatatosi che ciò a cui ad oggi non hanno potuto altri fattori di crisi, è arrivato a poterlo la crisi pandemica (essendosi passati da una situazione in cui dallo *smartphone* si voleva sapere *«what exactly your finger was clicking on»*, ad una in cui si vuole, inoltre, conoscere «*the temperature of your finger and the blood-pressure under its skin*»**[1]**).

Ma, più che in altre circostanze, ha generato sconcerto l'effetto sorpresa, che si auspica non debba più ripetersi nell'eventuale ripresentarsi di fenomeni simili. Ed anche per questo l'imperativo è quello di uno sforzo teso all'aggiornamento, grazie all'ausilio dello stesso progresso tecnologico, di strumenti di lavoro originatisi in altre epoche, in una prospettiva *constitutional oriented,* fermo restando l'*acquis* giuridico-culturale già maturato**[2]**.

2. *La fase I: la* App *tra Unione europea e Governo italiano*

La delicatezza di una tale situazione è stata immediatamente colta in ambito eurounitario, da parte, in particolare, dell'*European Data Protection Board* (nel prosieguo: EDPB), che, nel quadro della sua attività di promozione della cooperazione tra le autorità di protezione dei dati dell'Unione, ha prontamente evidenziato la necessità di mettere in campo «tecniche moderne» per la lotta contro il Covid-19, «nell'interesse dell'umanità»**[3]**; ammonendo, nel contempo, sul necessario rispetto, anche in contesti emergenziali, di tutti i diritti della persona, non ultimi quelli legati alla sfera di riservatezza individuale, protetti, com'è noto, espressamente dalla stessa Carta dei diritti fondamentali dell'Unione (artt. 7, 8 e 52).

È stato, del resto, su tale base, nonché tenendosi presenti le altre specifiche ed attuative discipline europee sulla protezione dei dati personali (spec. GDPR**[4]** e direttiva *e-privacy***[5]**), che sono stati dapprima enucleati e, dipoi, meglio specificati i principi fondamentali a cui gli Stati membri si sarebbero dovuti attenere: volontarietà, interoperabilità, copertura normativa, esplicitazione delle finalità, minimizzazione, trasparenza, protezione, pseudonimizzazione, sicurezza, temporaneità**[6]** (v. la tabella che segue).

I principi eurounitari in materia di applicazioni mobili per il contrasto al Covid-19

	European Data Protection Board (19 marzo)	**Commiss. UE Raccomandazione (8 aprile)**	**Commiss. UE Orientamenti e *Toolbox* Stati (16 aprile)**	**EDPB Lettera e Linee-guida (14 e 21 aprile)**
1. Volontarietà	Volontarietà	Volontarietà	Volontarietà Facoltatività No conseguenze neg^{ve}	Volontarietà Facoltatività No conseguenze neg^{ve}
2. Interoperabilità	Interoperabilità	Interoperabilità	Interoperabilità Coord. con autorità sanitarie Tit^{tà} autorità sanitarie naz^{li}	Interoperabilità Coord. con autorità sanitarie Tit^{tà} autorità sanitarie naz^{li}
3. Copertura normativa	“Legge”	“Legge”	“Legge” Necessarietà Proporzionalità Opportunità (efficacia)	“Legge” Necessarietà Proporzionalità Opportunità
4. Finalità	Finalità	Finalità	Finalità	Finalità
5. Minimizzazione	Minimizzazione	Minimizzazione	Minimizzazione	Minimizzazione Necessità Proporzionalità

6. Trasparenza	Trasparenza Informazione	Trasparenza Informazione Accessibilità	Trasparenza Informazione Accessibilità Codice sorgente
7. Protezione	Protezione Controllo dell'interessato Riservatezza Tutela dei dati Accesso, rettifica, cancellaz^{ne} No stigmatizzazione soc^{le}	Protezione Controllo dell'interessato Riservatezza Tutela dei dati Accesso, rettifica, cancellaz^{ne} No stigmatizzazione soc^{le}	Protezione Controllo dell'interessato Riservatezza Tutela dei dati Accesso, rettifica, cancellaz^{ne} No stigmatizzazione soc^{le}
8. Pseudonimizzazione	Pseudonimizzazione Aggregazione Anonimizzazione	Pseudonimizzazione Aggregazione Anonimizzazione Gestione separata dei dati	Pseudonimizzazione Aggregazione Anonimizzazione Gestione separata dei dati
9. Sicurezza	Sicurezza Autenticità Integrità	Sicurezza Autenticità Integrità	Sicurezza Autenticità Integrità Analisi d'impatto *Privacy by design* e *by default*

10. Temporaneità	Temporaneità Conservazione *in loco* Cancellazione Riesame periodico effvo	Temporaneità Conservazione *in loco* Cancellazione Riesame periodico effvo	Temporaneità Conservazione *in loco* Cancellazione Riesame periodico effvo Valutazione scientifica

Pertanto, quando, all'indomani della dichiarazione dello stato di emergenza[7], il nostro Paese si è inserito nel novero di quelli che andavano facendo ricorso ad una siffatta soluzione tecnologica, la "cornice normativa" era già stata ampiamente tracciata a livello sovranazionale, nella direzione della valorizzazione della tecnica di tracciamento. Di qui, pertanto, l'accantonamento, ad es., della tecnologia GPS, ultronea in quanto proiettata verso l'identificazione e geolocalizzazione degli utenti (*tracking*) a favore del *bluetooth Low Energy* con la sola rilevazione (*tracing*) dei contatti ravvicinati tra i dispositivi (v. *infra*, il §4).

Si deve, in particolare, all'allora Capo del Dipartimento della Protezione Civile il debutto, già con una delle proprie prime ordinanze, della progettazione dell'*App*, attribuendo, contestualmente, nel quadro della sua attività di coordinamento degli interventi nazionali per fronteggiare l'emergenza, la facoltà ai soggetti operanti nel Servizio nazionale di protezione civile "ed in via del tutto eccezionale" *anche* ad altri, di svolgere trattamenti di dati personali "particolari" concernenti lo stato di salute (art. 5 dell'ord. n. 3 del 2020)[8]. È stato poi il "Commissario Covid" nel frattempo nominato[9] ad affidare l'effettiva predisposizione dello strumento ad una società operante nel settore, con la previsione della stipula di un "contratto di concessione gratuita della licenza d'uso sul *software* e di appalto di servizio gratuito" (art. 6, c. 5 dell'ord. n. 10 del 2020)[10].

3. *La fase II: tra i due litiganti…*Google *ed* Apple *godono*

All'inizio della cd. "fase II", il nostro Paese ha potuto dunque essere ricompreso tra quelli che hanno optato per una applicazione mobile intesa al contrasto alla pandemia a basso tasso di intrusività[11]; sebbene, per vero, ancora poco di ufficiale si sapesse su come sarebbe funzionato il "Sistema Immuni" più ampiamente considerato (la stessa stipula del contratto di progettazione rimaneva in *standby*, in attesa di "indicazioni" più chiare[12]). Volendo azzardare un paragone,

si potrebbe dire che, in quel momento, dell'autovettura era noto l'impianto elettrico e la scocca, ma non ancora la carrozzeria ed il motore, né tanto meno il sistema di sicurezza. Sicché il parere espresso dal Garante dei dati personali**[13]** sulla proposta normativa predisposta all'uopo (contenute all'art. 6 del **d.l n. 28 del 2020[14]**) non ha potuto che in via interlocutoria essere positivo, consistendo i relativi rilievi in una serie di "raccomandazioni" sul "da farsi" circa, proprio, le specifiche tecniche che si fosse inteso adottare.

La situazione si è sbloccata all'indomani della decisione, da parte del nostro e di altri governi dell'UE, di abbandonare l'idea della predisposizione di una *App* (pan)europea "governata" dai singoli Stati (ed in prospettiva dall'UE) e, quindi, di tipo "centralizzato" (di tipo PEPP-PT), a favore dell'infrastruttura tecnologica di marca americana nel frattempo sviluppata e resa disponibile di concerto da *Apple* e *Google* (piattaforma A/G)**[15], che vedeva e vede, invece, *repository* e *data retention* gestiti dagli stessi** *smartphone,* secondo una soluzione considerata "decentralizzata" (DP-3T e soluzione A/G). Per cui la nuova architettura informatica ha determinato una differente modalità di trasmissione e conservazione dei dati degli utenti, dato che mentre con la soluzione centralizzata essi sarebbero stati gestiti, appunto, dal server centrale (nazionale), invece nella nuova struttura decentralizzata i medesimi vengono amministrati in via normale (ma cfr. *infra*, i §§ che seguono) in locale sullo *smartphone* (v. lo schema che segue).

imminui

L'impianto del *Sistema Immuni* conta, pertanto, ad oggi tre componenti fondamentali: la *App* installata sugli *smartphone*, il server nazionale ubicato presso il Ministero e la piattaforma situata, invece, oltre Atlantico, le quali, come vedremo, intervengono nel corso delle due delicate fasi in cui si svolge la procedura: quella "*ante alert*" (v. il §4) e quella "*post alert*" (v. il §6) di rischio contagio.

La novità non è stata scevra di problematicità sul piano normativo, perché sebbene dal legislatore fosse stata prospettata la possibilità di conservare i dati relativi ai contatti stretti "anche" nei dispositivi mobili degli utenti (art. 6, lett. *e)*, d.l. n. 28 del 2020, cit.), la stessa normativa sembrerebbe presupporre un impianto centralizzato, là dove prevede che *la* piattaforma informatica per la gestione del sistema di allerta debba essere "unica" e "nazionale" (art. 6, c. 1, d.l. n. 28 del 2020, cit.), nonché realizzata dal Commissario "esclusivamente con infrastrutture localizzate sul territorio nazionale" (art. 6, c. 5, d.l. n. 28 del 2020, cit.). Senza dire poi che la stessa *società chiamata a sviluppare la App è stata selezionata proprio in ragione della appurata idoneità a garantire la predisposizione di uno strumento conforme "al modello europeo delineato dal Consorzio PEPP-PT"***[16]**.

Che, poi, la questione abbia una portata che oltrepassa i confini nazionali, è dato di vedere nella pervicace volontà di alcuni Stati europei (spec. Francia[17]) di continuare a puntare sul "modello centralizzato" *al fine di preservare la propria "sovranità tecnologica"*[18], finendosi, peraltro, con ciò, non senza un qualche paradosso, per intralciare l'**interoperabilità dei sistemi operativi nella stessa aerea europea**[19]. Per altro verso, mentre i due colossi americani vanno affermando la propria tecnologia in Europa, il versante asiatico sembra procedere per proprio conto sostanzialmente incurante dell'interesse comune allo sradicamento dell'epidemia[20].

4. *La fase III: …tornando dalla App personale di* tracing

È opportuno ora soffermarsi su una delle principali ragioni che avrebbero motivato la scelta di deviare rispetto allo schema di *governance* iniziale: e cioè la ritenuta migliore idoneità di una siffatta soluzione proprio a «tutelare con maggiore forza la *privacy*»[21]. Sebbene, una tale considerazione sia stata motivata dall'impossibilità che vi sarebbe stata di allestire **"*in house*" una struttura tecnologica altrettanto affidabile in** tempi così ravvicinati[22], nondimeno, della stessa meritano in ogni caso di essere esaminati gli esiti, nella non abbandonata ipotesi dell'adozione, nel prossimo futuro, di una soluzione a tutti gli effetti "europea".

Ora, del tasso di intrusività della tecnologia *bluetooth* e, di conseguenza, della *App* isolatamente considerata si è detto (v. *supra,* il §2), restando, invece, da indagarne l'impiego nel quadro del Sistema Immuni ampiamente riguardato, alla luce, in particolare, delle specifiche tecniche (spec. dell'*Application Programming Interface-API*) intervenute strada facendo[23].

Nella cd. "fase II" si è appreso, dunque, che la riservatezza individuale dovrebbe essere garantita, *in primis*, "*by design*" oltre che dall'impossibilità di accedere ai dati personali contenuti nello *smartphone* dalla previsione dell'invio di un pacchetto di informazioni personali collegato ad un doppio scambio di codici parimenti pseudonimizzati. Ciò con l'obbiettivo di impedire la ricombinazione degli identificativi pseudonimizzati con le chiavi di co-decodifica necessari al *tracing****[24]*** e, più in generale, con tutte quelle "informazioni aggiuntive" (spec. di tipo biometrico, oltre che anagrafiche[25]), meglio idonee al *tracking,* in quanto in grado di risalire all'identità degli utenti[26].

Quanto, dunque, alla prima parte del processo tecnologico di *contact tracing* (v., *infra*, al § 6, la seconda parte), il contatto con gli altri *smartphone,* col relativo scambio dei dati e metadati[27] cifrati (che vengono poi memorizzati dagli stessi *smartphone*) avvengono attraverso identificativi casuali, pseudonimizzati ed altamente dinamici (i *Rolling Proximity Identifier-RPI*) avvicendantisi

di frequente[28]; i *RPI*, a loro volta, vengono prodotti a partire da chiavi "secondarie" parimenti pseudonimizzate e casuali (i *Rolling Proximity Identifier Key-RPIK*), prodotte contestualmente da chiavi "primarie"(le *Temporary Exposure Key-TEK*) che sono di più lunga durata rispetto ai *RPI* [29]...il tutto da parte di algoritmi crittografici elaborati dal *backend* del sistema.

In questo quadro, a mettere particolarmente a rischio il suddetto "disaccoppiamento" dei dati di *tracing* da quelli concernenti l'identità degli utenti è la cd. "reidentificazione inferenziale" (spec. dei soggetti risultati positivi) da parte di quegli "*App users*" (o, più in generale, di quei soggetti) che, essendo in possesso di "informazioni aggiuntive" di vario tipo, possono ricostruire a ritroso la propria "catena" di contatti sino ad arrivare ad individuare la persona all'origine del contagio. Di qui il monito del Garante «di evitare le occasioni» in cui i suddetti identificativi di prossimità e pseudonimi di breve periodo inviati in *broadcast*, «possano essere rilevati da terzi[30]», ed associati ad altre informazioni identificative dell'utenza, a maggior ragione se risultate positive al test[31]. Se quanto appena considerato (a tacere di più generiche forme di *hackeraggio*) fa ritenere «improbabili, ma non impossibili»[32] attacchi di de-anonimizzazione che, per l'appunto, consentono di identificare l'utente associato a un insieme di pseudonimi, ad aggravare ulteriormente la situazione potrebbe essere l'elevato grado di vulnerabilità della stessa tecnologia *bluetooth* che, pur costituendo la base del sistema (v., *supra,* il §2) non costituirebbe «un protocollo particolarmente robusto[33]». Anche se poi, a ben vedere, l'insidia di maggior momento dell'architettura decentralizzata, potrebbe essere data dall'alto tasso di esposizione al rischio di furto e smarrimento dei *device**[34]**,* data la moltiplicazione delle occasioni di *leakage* indotta delle stesse informazioni personali.

Per contro, è doveroso osservare come di analoghe fragilità non vadano esenti nemmeno i sistemi centralizzati, dovendo mettersi, sul piatto della bilancia, altresì, la constatazione della miniera di dati che in "un sol colpo" potrebbero esservi carpiti a seguito di un *data breach* ben mirato nell'ambito di un'architettura "unificata"[35]. Di qui la convenienza, sul piano metodologico, di limitare le verifiche al caso concreto in rapporto al tipo di dato ed all'infrastruttura tecnologica su cui si deve fare affidamento.

5. ...per andare alla *piattaforma multinazionale di* tracking

Va considerata ora la grande quantità di informazioni personali di cui entrano in possesso i gestori del Sistema Immuni, concernenti la vita reale come la *second life* digitale dei propri

utenti, data la possibilità, loro riconosciuta in via legislativa, di raccogliere dati ulteriori (spec. i cd. *analytics*), per il tramite degli stessi *device*, per fini di sanità pubblica e di miglioramento del sistema di allerta (art. 6, c. 1, d.l. n. 28 del 2020, cit.); per non dire della disponibilità di altre informazioni altamente identificative degli utenti (*mac address* del *bluetooth*, gli IP *address* ed i codici IMEI degli *smartphone*, solo per citarne alcuni)**[36]**.

Il quesito allora s'impone se sia adeguato e sufficiente un atto di fiducia**[37]** nei confronti di soluzioni, per di più, estranee alla giurisdizione europea, per escludere che attraverso l'impiego di appositi algoritmi combinatamente ad altre tecniche (come il *machine learning*), sugli stessi *analytics***[38]** e più ampiamente ancora sui *big data***[39]** attinti, *in primis*, dagli stessi *smartphone*, si renda possibile non solo risalire all'identità degli utenti, ma financo dei medesimi profilare la persona e personalità, condizionandone, altresì, il comportamento**[40]**.

Alla domanda, infatti, non potrebbe non rispondersi riproponendo il problema della "controllabilità dei controllori", data la difficoltà di vigilare sul fatto che in particolare i gestori extraeuropei non utilizzino indebitamente le informazioni a propria disposizione, specie le chiavi di decriptazione dei dati personali pseudonimizzati che transitano e vengono stivati nell'ambito del sistema Immuni (v. *supra*, i §§3 e 4).

Si comprende, tra l'altro, lo scrupolo del Garante nel prevenire ogni forma di riassociazione degli stessi *analytics* «a interessati identificabili», assicurando, nel contempo, «l'adozione di adeguate misure di sicurezza e tecniche di anonimizzazione», nel rispetto dei principi di *privacy by design* e *by default* (di cui all'art. 25 del GDPR)**[41]**. Ma, soprattutto, non andrebbero in questa stessa prospettiva trascurati gli *input* provenienti (anche) dalla stessa Unione europea, circa l'importanza (tramontata definitivamente l'idea di poter "*be alone*" ed ancora in attesa dei necessari anticorpi tecnologici) di "*be informed*", dotandocisi di un adeguato apparato competenziale e culturale, onde scongiurare il diffondersi di un altrimenti possibile analfabetismo tecnologico "di ritorno". Per cui è, per l'appunto, nell'ottica della trasparenza e conoscibilità (oltre che nella prospettiva di uno sviluppo tecnologico condiviso), che, a chi domina il sistema, si chiede di rendere disponibili in forma gratuita e con licenze *open source* i codici sorgente dei programmi informatici, nonché il rilascio di precise informative dei meccanismi di funzionamento delle medesime tecnologie e dei diritti dei soggetti interessati dai relativi trattamenti di dati (secondo, del resto, la filosofia propria delle norme europee in materia)**[42]**.

È, del resto, su simili premesse che, tornando a quanto si diceva riguardo al sistema Immuni, ad *Apple* e *Google* si è reclamato di meglio chiarire, in particolare, le caratteristiche degli algoritmi di calcolo utilizzati (spec. per la valutazione del rischio di esposizione al contagio), la portata dei *bug* di sistema presenti (spec. quanto alla generazione di "falsi positivi" e "falsi negativi"), nonché le autorizzazioni di accesso al sistema (spec. quanto ai possibili interventi degli amministratori dei sistemi operativi, sulla rete e sulle stesse basi dati)….precisandosi, altresì, i rispettivi ruoli, «in ossequio ai principi di trasparenza e responsabilizzazione»**[43]**.

6. …passando *dal server nazionale di* testing *ed* identification

Tornando al versante infrastrutturale, va portata attenzione all'ulteriore crocevia di informazioni che, specie in prospettiva, potrebbe essere il "server" (*rectius*: la "piattaforma", nelle intenzioni del legislatore) del Ministero della Salute, in capo al quale è stata posta la titolarità del trattamento dei dati nel quadro del Sistema Immuni (art. 6, c. 1, d.l. n. 28 del 2020, cit.).

È, infatti, lo stesso dato normativo a prevedere la "complementarietà" delle "modalità operative del sistema di allerta tramite la piattaforma informatica" alle ordinarie modalità in uso nell'ambito del Servizio sanitario nazionale (art. 6, c. 1, d.l. n. 28 del 2020, cit.); acconsentendo, altresì, a che i dati raccolti attraverso l'applicazione possano essere utilizzati "in forma aggregata o comunque anonima", per fini di "sanità pubblica, profilassi, statistici o di ricerca scientifica" (art. 6, c. 3, d.l. n. 28 del 2020, cit.). A ciò vanno sommate, poi, le informazioni "aggiuntive" che potranno rendersi disponibili dall'innesto di *patch*, interconnesse, peraltro, con la sopra esaminata piattaforma straniera A/G (così da avere messo in agenda l'implementazione dei "diari clinici" degli utenti, mentre già si parla dell'implementazioni di "passaporti sanitari digitali" e delle "cartelle cliniche" dei pazienti)**[44]**.

Tanto più che a conferire al Ministero un ruolo sul piano puramente giuridico, al momento comparabile a quello che il binomio A/G ha su quello tecnologico, è il fatto che, già oggi, si tratta del (solo) soggetto a cui è legittimamente consentito di conoscere l'identità delle persone risultate positive al Covid-19.

Gli operatori sanitari del SSN sono, infatti, ad oggi, i soli ai quali, a quanto ci consta, risulta possibile rivolgersi ed a cui, in questi casi**[45]**, è necessario fornire le proprie anagrafiche, appartenendo ad essi il delicato compito di "attestazione", a partire da quel momento, della correttezza della procedura**[46]**. Dal che, sebbene viga l'obbligo di segretezza, la evidenziata «

potenziale collusione» tra l'entità che rileva la positività del paziente e il sistema di gestione dei server che gestiscono il *proximity tracing*[47].

Venendo dunque alla seconda parte del processo tecnologico (v., *supra*, al §4 la prima), il Sistema Immuni è programmato in modo tale da aversi una connessione periodica in automatico degli *smartphone* ad un *Diagnosis Server* gestito dallo stesso Ministero della Salute (v. *infra*) con lo scambio tra gli *smartphone* degli identificativi giornalieri TEK di cui si è detto, associati ai casi risultati positivi e la verifica della loro eventuale "corrispondenza" con la lista dei RPI memorizzati dagli stessi *smartphone* nel periodo di riferimento (v. *supra*, il §4). A questo punto, in caso di esito positivo, è il *software* A/G a fare, per così dire "da collante" tra le varie componenti del sistema consentendo il percorrimento "a ritroso" delle tappe compiute nella prima parte del processo (derivazione dalle TEK delle RPIK e da esse, quindi, gli identificativi temporanei RPI), al fine di risalire al *device* di riferimento a cui inviare l'*alert* di contagio. A questo punto le persone destinatarie dei relativi *alert* possono a loro volta decidere di sottoporsi ai controlli sanitari al fine di verificare il proprio stato di salute, rivolgendosi quindi, in caso di esito positivo, agli operatori sanitari, secondo un processo circolare che per noi, a questo punto, si chiude[48].

Come si vede, il meccanismo ed il flusso di informazioni che vengono messe in moto dal sistema necessitano di un'infrastruttura tecnologica solida ed di un'organizzazione amministrativa strutturata, trattandosi delle condizioni basilari per il conseguimento degli obbiettivi di efficacia e GDPR *compliance*. Sembra però lecito nutrire qualche dubbio al riguardo, data la disorganicità che, al momento, affligge l'impianto chiamato a tenere la regìa delle cose in ambito interno. In particolare, al momento non risultano del tutto perspicue le specifiche sulla base delle quali il Ministero dell'economia e delle finanze, insieme ad un'azienda operante nel settore dell'ICT (*in house*), in qualità di responsabili del trattamento, procedono, a supporto dello stesso Ministero della Salute[49], all'erogazione del servizio di interazione con gli operatori sanitari[50]. Inoltre, al momento, non paiono nemmeno chiare le specifiche tecniche e giuridiche in cui agiscono gli ulteriori fornitori di servizi sul territorio che (una volta accantonata l'idea di far convergere direttamente il flusso di dati sul server "centrale") in qualità di "subresponsabili" dei trattamenti di dati, sono chiamati a mettere a disposizione la propria rete di distribuzione dei contenuti in varie parti del territorio nazionale (il *Content Delivery Network*)[51] quali "nodi di prossimità" tra il centro (il Ministero della Salute) e la periferia (gli *smartphone*)[52].

7. *Una "costituente tecnologica" eurounitaria (ed italiana)?*

Difficile tentare ora conclusioni anche sommarie data la fluidità della situazione, ma dalla vicenda Immuni sembra comunque confermata la stretta interrelazione tra *governance* politica ed infrastruttura tecnologica, non senza ricadute sulla tutela di diritti fondamentali (legati, in partic., alla sfera della *privacy*).

Il ritardo, inoltre, dell'Unione europea e degli Stati membri rischia di farsi irrimediabile se non si procede celermente alla messa a punto anche di un'"Unione digitale"**[53]** e all'approntamento di una piattaforma comune ("paneuropea"), solida e capillarmente diffusa tra i vari Stati membri, su cui addensare le informazioni di carattere personale**[54]**. Una tale cessione di "sovranità digitale" da parte degli Stati membri, mentre, dunque, nell'immediato, potrebbe verosimilmente contribuire a colmare lo scarto tra la debolezza infrastrutturale ed invece la "forza" del dato normativo eurounitario in materia, nel più lungo periodo, potrebbe fare da contrappeso al solidificarsi di monopoli tecnologici su scala globale**[55]**.

Dinnanzi alla situazione attuale, che vede sostanzialmente la vigenza di due modelli di *governance* tecnologica (anche) dei dati personali – uno "a gestione autoritaria", in mano a poteri pubblici non democratici nel senso invalso nella tradizione costituzionalistica occidentale (v. Cina) ed un altro, invece, "a gestione indipendente", rilasciata completamente nella disponibilità di soggetti privati (Stati Uniti) – l'auspicio sarebbe che un'Unione tecnologica europea coltivi la sua connaturata via di una "gestione democratica" dell'infrastruttura e dei trattamenti.

In questo scenario, guardandosi all'Italia, risulta, a maggior ragione, valida la speranza che proprio verso una "sana" gestione dell'infrastruttura tecnologica vengano subito indirizzate energie e risorse. Di fronte al contagio, infatti, il nostro Paese si è trovato nelle condizioni di doversi affidare a soluzioni "miste" non del tutto compiute, scommettendo su un sistema di allerta, dalla (inter)faccia apparentemente "*soft*", nell'ambito di una base giuridica (non repressiva ma) puramente volontaria e solidaristica. Così tuttavia, non è senza un qualche paradosso che ci si trova esposti al rischio di vedere pregiudicati i principali valori in campo: *privacy* e salute individuale e collettiva**[56]**, con una compromissione complessiva del livello delle tutele di diritti fondamentali**[57]**.

[1] Così Y.N. Harari, *The world after coronavirus,* in ***www.ft.com*** del 20 marzo 2020.

[2] Con più specifico riguardo "alla rotta", indicata dal Presidente della Corte costituzionale, nel pieno dell'emergenza, si rinvia all'intervista di L. Milella, *Cartabia: "La Costituzione una bussola nell'emergenza. Non c'è diritto speciale per tempi eccezionali"*, in ***www.repubblica.it*** del 28 aprile 2020.

[3] EDPB, ***Dichiarazione sul trattamento dei dati personali nel contesto dell'epidemia di COVID-19***, del 19 marzo 2020, 1.

[4] Ci si riferisce, in partic., al Reg. UE del 27 aprile 2016, n. 679 (GDPR), "on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC" (spec. i consid. n. 35, n. 41, n. 46, n. 51, n. 53 e n. 54, nonché gli artt. 4, 6 e 9).

[5] Ci si riferisce, in partic., alla dir. 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, "relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche" (spec. gli artt. 6, 9 e 15).

[6] Commiss. EU, **Racc. (UE)** 2020/518 dell'8 aprile 2020 "relativa a un pacchetto di strumenti comuni dell'Unione per l'uso della tecnologia e dei dati al fine di contrastare la crisi Covid-19 e uscirne, in particolare per quanto riguarda le applicazioni mobili e l'uso di dati anonimizzati sulla mobilità" (C/2020/3300); EDPB, **Lettera** alla Commissione recante il "Progetto di Linee-Guida per app di contrasto alla pandemia COVID-19", del 14 aprile; Commiss. EU, **Comunic.** "Orientamenti sulle app a sostegno della lotta alla pandemia di covid-19 relativamente alla protezione dei dati", del 17 aprile 2020); e, quindi, nuovamente, EDPB, **Linee guida** "sull'utilizzo della geolocalizzazione e di altri strumenti di tracciamento nel contesto dell'emergenza legata al Covid-19", del 21 aprile 2020.

[7] V. la **Delibera** del Consiglio dei ministri del 31 gennaio 2020, di "Dichiarazione dello stato di emergenza in conseguenza del rischio sanitario connesso all'insorgenza di patologie derivanti da agenti virali trasmissibili" CORSIVO?.

[8] V. l'**ocdpc** del 3 febbraio 2020, n. 630 recante i "Primi interventi urgenti di protezione civile in relazione all'emergenza relativa al rischio sanitario connesso all'insorgenza di patologie derivanti da agenti virali trasmissibili" CORSIVO?, a cui, il giorno prima, il Garante per la protezione dei dati personali aveva dato "via libera" (v. il **Parere** n. 15 del 2 febbraio 2020).

[9] V. il **dPCM** del 18 marzo 2020 di "Nomina del dott. Domenico Arcuri a Commissario straordinario per l'attuazione e il coordinamento delle misure occorrenti per il contenimento e

contrasto dell'emergenza epidemiologica COVID-19".

[10] V. l'**ord. del 16 aprile 2020, n. 10**, del Commissario straordinario per l'attuazione e il coordinamento delle misure di contenimento e contrasto dell'emergenza epidemiologica covid-19, con cui si è disposto "di procedere alla stipula del contratto di concessione gratuita della licenza d'uso sul *software* di *contact tracing* e di appalto di servizio gratuito con la società Bending Spoons S.p.a.".

[11] Come puntualmente notato, all'epoca, da T. Frosini, ***Anonimato, privacy, niente obbligo: le salvaguardie ora ci sono***, *Il Dubbio* del 5 maggio 2020.

[12] V.lo alla nota 16.

[13] V. Garante per la protezione dei dati personali, **Parere** sulla proposta normativa per la previsione di una applicazione volta al tracciamento dei contagi da COVID-19 del 29 aprile 2020.

[14] Trattasi, per la precisione, dell'art. 6 recante "Misure per l'introduzione del sistema allerta Covid-19", del **d.l.** del 30 aprile 2020, n. 28, recante "Misure urgenti per la funzionalità dei sistemi di intercettazioni di conversazioni e comunicazioni, ulteriori misure urgenti in materia di ordinamento penitenziario, nonché disposizioni integrative e di coordinamento in materia di giustizia civile, amministrativa e contabile e misure urgenti per l'introduzione del sistema di allerta Covid-19". Si precisa che il testo della relativa legge di conversione è stato approvato al Senato (il 17 giugno 2020) epperò, al momento in cui si scrive, è ancora in corso di esame in commissione alla Camera dei deputati.

[15] Il Ministero dell'Innovazione avrebbe proceduto alla pubblicazione del codice *backend* della *App* relativo all'elaborazione ed alla trasmissione dei dati personali sulla piattaforma ***Github*** il 25 maggio 2020.

[16] *Così da rendere* in corso d'opera necessario "calibrare" le clausole del **contratto** che sarebbe stato stipulato il 16 maggio 2020 dal Commissario straordinario per l'attuazione e il coordinamento delle misure di contenimento e contrasto dell'emergenza epidemiologica Covid-19 con la Bending Spoons S.p.A. (v. spec. l'Allegato 2: "Attività di miglioria e personalizzazione dell'App": "Modifica al sistema di caricamento dei dati dell'utente, sfruttando sistemi di sblocco diversi da quello attualmente previsto dal modello PEPP-PT").

[17] Sul "modello misto" e "proprietario" che si sta predisponendo in Francia, cfr., ad es., V. Iovino, **Contact tracing, *la Francia si disallinea: ecco la sua "terza via"***, del 1°giugno 2020; per un panorama più ampio della situazione cfr., invece, "agli esordi" ad es. R. Angius e L.

Zorloni, ***Coronavirus e contact tracing, cosa fanno gli altri stati in Europa***, del 18 aprile 2020; e M. Notarianni, ***Sette nazioni EU scelgono l'approccio Apple e Google per il tracciamento Covid-19***, del 7 maggio 2020.

[18] Cfr., sia pur da un angolo visuale più specifico, G. Pitruzzella, O. Pollicino, Disinformation and hate speech. A European Constitutional Perspective, Milano, 2020.

[19] Cfr., sul punto, B. Calderini, ***App coronavirus, funzioneranno all'estero? Il dilemma interoperabilità***, del 21 maggio 2020.

[20] Un tale scenario motiva, dunque, comprensibilmente, l'attenzione riservata alla vicenda dal Comitato parlamentare per la sicurezza della Repubblica (Copasir), segnatamente il rilievo che vi fossero rischi geopolitici non trascurabili, che avrebbero necessitato di vedere monitorato il fatto che nessuno potesse e possa accedere ai dati (cfr., *ex multis*, G. Postiglione, ***Se neanche lo Stato si fida di sé stesso***, del 12 giugno 2020.

[21] V., in tal senso, già C. Rossi, ***App Immuni, consorzio Pepp-Pt e Bending Spoons: fatti, obiettivi, analisi e polemiche*** del 19 aprile 2020; ed in seguito, A. Longo, ***L'app Immuni cambia. Seguirà il modello decentralizzato di Apple e Google Una scelta ormai definitiva. E anche obbligata. per tutelare con maggiore forza la privacy e la sicurezza dei dati*** del 22 aprile 2020; e A. Cazzullo, ***Coronavirus, Colao: «Un'apertura a ondate per testare il sistema. L'app entro maggio oppure servirà a poco»***, del 29 aprile 2020.

[22] Così lo stesso Garante per la protezione dei dati personali, ***Provvedimento di autorizzazione al trattamento dei dati personali effettuato attraverso il Sistema di allerta Covid-19 - App Immuni*** del 1° giugno 2020.

[23] Per la precisione, le API sono state rese disponibili nella seconda metà di maggio (cfr., al riguardo, ad es., L. Garofalo, ***Disponibili le API di Apple e Google Conte***, del 21 maggio 2020). V., inoltre, *supra*, la nota 15.

[24] Segnatamente, di ricalcolare le chiavi RPIK a partire dalle RPI e/o le chiavi TEK a partire dalle RPIK.