

CONTACT TRACING E PROTEZIONE DEI DATI NELLA FASE 2 DELL'EPIDEMIA DA COVID-19 (ANCHE NEL RAPPORTO DI LAVORO)

di **LUCIA D'ARCANGELO**

Articolo del 08 maggio 2020

ISSN 2420-9651

L'individuazione delle misure di prevenzione del contagio del rischio Covid-19 che tutte le imprese dovranno adottare, sia quelle che sono in procinto di riaprire, sia quelle che non hanno sospeso le attività, è tema di discussione tra i giuslavoristi [v. gli Autori indicati in bibliografia], ma ad esso rivolge attenzione pure la stampa quotidiana attratta da qualche grande azienda che ha già messo in campo alcuni interessanti modelli di sicurezza.

SOMMARIO: 1. Sicurezza sul lavoro e privacy: un binomio possibile? - 2. Il contact tracing: come e quando. - 3. Contact tracing e dati personali. - 4. L'app Immuni e la limitazione del diritto di tutela dei dati al vaglio del test di proporzionalità. - 5. Rilievi sul tracciamento dei contatti con riferimento alle Linee-guida dell'Edpb (European Data Protection Board) del 21 aprile 2020. - 6. Riferimenti bibliografici.

1. Sicurezza sul lavoro e privacy: un binomio possibile?

L'individuazione delle misure di prevenzione del contagio del rischio Covid-19 che tutte le imprese dovranno adottare, sia quelle che sono in procinto di riaprire, sia quelle che non hanno sospeso le attività, è tema di discussione tra i giuslavoristi [v. gli Autori indicati in bibliografia], ma ad esso rivolge attenzione pure la stampa quotidiana attratta da qualche grande azienda che ha già messo in campo alcuni interessanti modelli di sicurezza.

Pioniere sono le case automobilistiche Ferrari e Fiat Chrysler con la scelta di progetti *testing-tracking*, basati su *test* sierologici rapidi e su sistemi di tracciamento digitale dei contatti, insieme alle linee guida “condivise tra le Parti per agevolare le imprese nell'adozione di protocolli di sicurezza anti-contagio” contenute nel **Protocollo per il contrasto e il contenimento della diffusione del virus Covid-19 negli ambienti di lavoro** (con riferimento specifico a quelli non sanitari) siglato dalle organizzazioni sindacali su impulso del Governo lo scorso 14 marzo 2020 [Dagnino 2020] e **integrato il 24 aprile 2020**

(<https://www.uilmnazionale.it/wp-content/uploads/2020/04/20200424-DOCUMENTO-PROTOCOLLO-SICUREZZA-Cgil-Cisl-Uil-Mise-e-M-Salute-Min-Lav.pdf>).

Non ci si sofferma sui contenuti del Protocollo ma si apre solo una brevissima parentesi per mettere in risalto che *sia* le regole per consentire l'ingresso in azienda (fra le varie spicca il punto 2: misurazione della temperatura corporea) *sia* gli strumenti *testing* (*test* sierologici rapidi), danno luogo ad accertamenti sanitari che si pongono in deroga con [l'art. 5 dello Statuto dei lavoratori](#) giacché saranno effettuati direttamente dal datore di lavoro che li eseguirà tramite il medico competente [Carinci 2020, 8 ss.], come infatti è preannunciato tra le nuove integrazioni dell'accordo sindacale ove si evidenzia una intensificazione significativa dei compiti spettanti a tale figura.

Riguardo alle menzionate aziende automobilistiche ci si limita ad evidenziare che mentre Fiat Chrysler ha già firmato un accordo con le organizzazioni sindacali nazionali (Fca, fim, Uilm, Fismic, Uglm, Aqcfr, fiom, 9 aprile 2020) che contiene indicazioni in linea con le linee guida del Protocollo dello scorso 14 marzo, - e che dovrà aggiornare alla luce delle integrazioni appena apportate dalle parti sociali – Ferrari, invece, si è spinta oltre l'applicazione delle regole concertate in sede sindacale, prevedendo *screening* sulla salute dei lavoratori attraverso la somministrazione di *test* sierologici rapidi, che sembrano idonei a rivelare i cd. portatori asintomatici, e modalità di

tracciamento dei dipendenti medesimi per contenere l'espansione del virus.

Da quanto si apprende dalle testate giornalistiche (le fonti di informazione sono varie, non sempre univoche e in continuo aggiornamento, con tutti i limiti che ne derivano in termini di attendibilità), la casa automobilistica sarebbe dell'idea di privilegiare **un'applicazione digitale**, forse **Immuni**, quellache il governo italiano ha selezionato per l'avvio della fatidica fase 2, almeno così pare (non a caso la società proponente sembra essere Bending Spoons, la stessa). Lo scopo, a dire dell'azienda, sarebbe di monitorare nei mesi prossimi l'evoluzione del virus in azienda e fornire supporto medico sia ai lavoratori che ai loro familiari e anche al personale fornitore dell'azienda. E' sull'app Immuni e, prima ancora, sul *tracking*, che concentriamo l'attenzione, dopo aver premesso che il tracciamento digitale sul luogo di lavoro comprende una vasta gamma di tecnologie che si risolvono in forme di controllo a distanza dei lavoratori attuabili con sistemi *wearable device*, quali *smartwatch* o altri *smart sensor*, braccialetti elettronici o, appunto, con app scaricabili sul *smartphone*. Le quali si ritiene possano trovare collocazione nell'art. 4, dello Statuto, in particolare al comma 1, nell'ambito della categoria degli “altri strumenti”che possono essere impiegati, al fianco degli impianti di videosorveglianza e degli strumenti di lavoro, per finalità di “sicurezza del lavoro”, naturalmente previa mediazione sindacale e/o amministrativa.

E' necessario, tuttavia, avere contezza che dietro tali strumentazioni tecnologiche si insinuano forme inedite di controllo, non solo all'interno dell'ambiente di lavoro ma, prima ancora, al di fuori di esso.

Per questa ragione analizziamo il fenomeno del *contact tracing*, con riferimento specifico alle conseguenze della sua implementazione sulla disciplina del trattamento dei dati personali, anche in considerazione, nel prossimo futuro, di un possibile effetto emulativo, da parte di altre realtà aziendali, delle scelte manageriali oggi compiute in casa Ferrari con l'uso, probabilmente, come si è detto, dell'applicazione Immuni.

2. Il contact tracing: come e quando.

La premessa da cui partire, nella prospettiva che si intende illustrare, è la seguente: se rallentare la diffusione di un *virus* epidemico è un esercizio di democrazia, l'audacia restrittiva delle misure limitative delle libertà personali costituzionalmente garantite va rispettata nei limiti di quella temporaneità dovuta all'emergenza, che ogni Stato di diritto è tenuto ad assicurare per “non (...) consolidare compressioni definitive di alcun diritto”

[Epidiando 2020, 5].

L'esigenza di tutela della salute pubblica, quale diritto individuale e interesse collettivo, nella geometria dei valori costituzionali, ha prevalso, nel contesto della crisi sanitaria in corso, sulle prerogative di salvaguardia della società nei suoi aspetti economici, civili, politici, almeno fino ad ora. Ma la dialettica tra i diritti fondamentali della persona è in procinto di scatenarsi, compatibilmente con la prefigurazione, da parte degli esperti, dell'attenuarsi dell'epidemia in ambito nazionale, perché diventa indispensabile stabilire i parametri della convivenza con il virus Covid-19, almeno in attesa della soluzione vaccinale.

Il **contact tracing** è una delle misure previste per l'avvio della cosiddetta fase 2 della epidemia che consiste nella georeferenziazione dei contagiati e di coloro con cui si sono avuti possibili contatti. In pratica, un'applicazione digitale, sfrutta i dati di geolocalizzazione presenti sugli *smartphone* e attraverso un sistema di intelligenza artificiale riesce ad individuare gli spostamenti delle persone, i luoghi frequentati da chi è stato contagiato, permettendo di risalire ai cittadini oggetto di contatto. Così, sappiamo, si è fatto in Cina, Corea del Sud, Singapore, poi anche Israele e da ultimo persino in Albania, ma sul piano civile e politico si registrano alcune perplessità riguardo all'implementazione italiana, in parte dovute alle nostre differenze con quei regimi di governo [Cuocolo 2020, 5-7; 12 ss.], specie quello cinese e coreano.

Nel vantaggio, infatti, di ripristinare, *medio tempore*, la produttività economica e sociale del Paese, risiede anche il pericolo che venga “messa a nudo” la persona e la sua sfera d'azione, il che significa, sul piano giuridico, che può essere scalfito il modello di tutela dei dati personali da poco in vigore in Italia -e negli altri paesi d'Europa- contenuto nel [Regolamento Ue 2016/679](#) e nel [d.lgs. 196/2003](#), come modificato dal [d.lgs. n. 101/2018](#).

A ciò si potrebbe obiettare che i nostri dati sono già in possesso delle multinazionali digitali, che siamo geolocalizzati tramite la segnalazione della posizione su Google, difatti la mappa degli spostamenti è già ora ricostruibile utilizzando i dati forniti da Google, Facebook, Apple. Benché sia pure vero che con la semplice disattivazione della posizione si interrompe la tracciabilità e di conseguenza viene meno il rischio di un trattamento indebito delle informazioni sui nostri spostamenti.

Il problema, allora, è di capire se il tracciamento digitale che allo stato si prevede di adottare tramite l'applicazione Immuni, e che sarà scaricabile su base volontaria

sfruttando la tecnologia *bluetooth* in grado di rilevare la vicinanza tra due *smartphone* nell'arco di un metro di distanza, così da poter rintracciare i possibili contagiati e isolarli, possa configurarsi come una misura idonea a controllare la dimensione evolutiva del fenomeno virale anzitutto dal punto di vista della sua legittimità giuridica nel nostro ordinamento.

3. Contact tracing e dati personali.

In sostanza, l'adozione dello strumento del *contact tracing* comporta una limitazione della nostra sfera personale, non palpabile nell'immediato, ma molto pervasiva, ovvero il monitoraggio, da parte delle multinazionali digitali (compagnie telefoniche e/o anche *social network*), delle nostre azioni e di tutto quel che riguarda la nostra persona, che rientra nel concetto di “diritto di protezione dei dati personali”.

Ricordiamo che il *right to protection of personal data*[Lattanzi 2014, 10] risponde all'idea, che è stata per prima dell'Europa e successivamente dei singoli Stati, di dare fondamento giuridico a quel concetto di riservatezza (*privacy*), diffuso da largo tempo e poi diventato d'uso comune, spesso in maniera anche smodata. Un diritto soggettivo che ha ad oggetto la tutela del dato personale, che il [Regolamento \(Ue\) 2016/679](#) identifica in “qualsiasi informazione riguardante una persona fisica identificata o identificabile, ove per “identificabile” si intende “la persona fisica che può essere identificata, direttamente o indirettamente” (art. 4). Come sia possibile l'identificazione ovvero la riconducibilità ad una persona è spiegato efficacemente nel **Considerando 30**: «Le persone fisiche possono essere associate a identificativi online prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli indirizzi IP, marcatori temporanei (cookies) o identificativi di altro tipo, quali i tag di identificazione a radiofrequenza. Tali identificativi possono lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone fisiche e identificarle».

Basta questo per rendersi conto di quanto sia facile, per chi pone in essere un'attività di tracciamento con strumenti digitali, travalicare la soglia della tutela del dato personale. Occorre, perciò, affrontare la questione da una duplice angolazione, verificando, in primo luogo, la **legittimità** del *contact tracing* nel quadro normativo delle fonti, con riferimento particolare alla disciplina sulla protezione dei dati, al fine di accertare,

subito dopo, i limiti di una eventuale “**comprimibilità**” della **legislazione sui dati personali**.

Riguardo al primo aspetto, sul versante della protezione dei dati, il [Regolamento \(Ue\) 2016/679](#) autorizza il trattamento di dati particolari (sensibili), in via derogatoria, al ricorrere di precise condizioni elencate all'art. 9, paragrafo 2: “per motivi di interesse pubblico nel settore della sanità pubblica” (lett. *g-i*), “diagnosi, (...) terapia sanitaria (...) gestione dei (...) servizi sanitari o sociali” (lett. *h*). Sulla stessa scia, il novellato [d.lgs. n. 196/2003](#), che considera di “rilevante interesse pubblico” i trattamenti eseguiti dal servizio sanitario nazionale e dai soggetti operanti in ambito sanitario, per la “sicurezza e salute della popolazione, protezione civile, salvaguardia della vita e incolumità fisica” (art. 2-*sexies*, comma 2, lett. *t-u*)).

Da questa stessa angolazione va esaminata anche la **decretazione d'urgenza del 9 marzo 2020, n. 14**, emanata nell'ambito della crisi sanitaria *in itinere*, sul tema del potenziamento del Servizio sanitario nazionale come simbolo dell’“intervento del potere pubblico in funzione di mediatore del conflitto all'interno dei confini costituzionali” [Caruso 2020], ora abrogata per effetto della **conversione in legge, con modificazioni, del decreto-legge 17 marzo 2020, n. 18**. Il testo del **disegno di legge approvato dal Senato il 9 aprile 2020** prevede l'inserimento di un nuovo **art. 17-bis**, in tema di trattamento di dati personali nel contesto emergenziale, che nella sostanza riproduce il contenuto dell'art. 14, d.l. n. 14/2020. Dal provvedimento, nel complesso, emerge che l'autorità politica ha mostrato particolare sensibilità nei confronti della disciplina sulla protezione dei dati personali, avendo disposto che i trattamenti di dati personali in genere, compresi quelli sanitari, devono essere eseguiti nel rispetto delle disposizioni del Regolamento sulla tutela dei dati appena menzionate. In modo particolare, che gli stessi possono essere considerati legittimi limitatamente alla “durata dell'emergenza sanitaria”, quando sono svolti da talune, specifiche, categorie di soggetti (operanti nei settori della sanità, della protezione civile, della pubblica sicurezza), infine, se sono ritenuti necessari per la difesa della salute pubblica. Peraltro, ha anche consentito “la comunicazione dei dati personali a soggetti pubblici e privati diversi da quelli di cui al comma 1, nonché la diffusione dei dati personali (...)” di genere comune ove risulti “indispensabile ai fini dello svolgimento delle attività connesse alla gestione dell'emergenza sanitaria in atto”.

Dunque, stando alla ricostruzione del dato normativo, sembra di poter convenire sulla

ammissibilità di un trattamento di dati nella forma del controllo digitale della persona e dell'intera società, se è in gioco la salute pubblica. D'altra parte è la coesistenza tra i diritti stessi ad imporne la rivalutazione nell'ottica di una ponderazione equilibrata quando si verificano situazioni di conflittualità. Ce lo ricorda la Corte costituzionale nella pronuncia sul caso Ilva quando afferma che «tutti i diritti fondamentali tutelati dalla Costituzione si trovano in rapporto di integrazione reciproca e non è possibile pertanto individuare uno di essi che abbia la prevalenza assoluta sugli altri. La tutela deve essere sempre “sistemica e non frazionata in una serie di norme non coordinate ed in potenziale conflitto tra loro” (...). Se così non fosse, si verificherebbe l'illimitata espansione di uno dei diritti, che diverrebbe “tiranno” nei confronti delle altre situazioni giuridiche costituzionalmente riconosciute e protette, che costituiscono, nel loro insieme, espressione della dignità della persona» ([Corte cost., 9 maggio 2013, n. 85](#), in *Giur. it.*, 2013, 3, 1424, con nota di Sereno; Bin; Pulitanò; Onida). Sicché è condivisibile ritenere che «Queste affermazioni, pronunciate allora per postergare il diritto alla salute al diritto al lavoro e alla libera iniziativa economica, vanno tenute a mente oggi, in un contesto assai diverso che vede rovesciata quella particolare relazione di precedenza» [Caruso 2020], attraverso la postergazione del diritto alla protezione dei dati personali al diritto e interesse collettivo della salute.

4. L'app Immuni e la limitazione del diritto di tutela dei dati al vaglio del test di proporzionalità.

Da questa seconda angolazione, occorre verificare fino a che punto si può comprimere il diritto di ciascuno alla tutela delle proprie informazioni per il bene della salute pubblica, muovendo dai principi generali applicabili ai trattamenti di dati, stabiliti dall'[art. 5 del Regolamento \(Ue\) 2016/679](#), i quali impongono che ogni raccolta di informazioni persegua obiettivi determinati, coincida con il tempo del loro raggiungimento e, soprattutto, risulti a ciò necessaria (“limitazione delle finalità”, “limitazione della conservazione” e “minimizzazione dei dati”). Ne consegue, che, una volta tracciate le informazioni utili a contenere l'espansione della malattia virale, queste non possono essere conservate oltre il tempo necessario alla salvaguardia della salute collettiva, che, come si è detto all'inizio, si deve presumere possa limitarsi all'attesa della risposta farmacologica di natura prevenzionale.

Più precisamente, vuol dire che il trattamento di raccolta deve soddisfare il principio di

proporzionalità, valutazione, quest'ultima, che è stata affrontata in varie occasioni dai giudici comunitari, sebbene con operazioni di bilanciamento tra diritti fondamentali non sempre sufficientemente argomentate secondo una logica precisa (C. giust. UE, grand. sez, 24 settembre 2019, C-507/17 e 24 settembre 2019, C-136/17, entrambe in *Foro it.*, 2019, 12, IV, 572; C. giust. UE, grand. sez, 13 maggio 2014, C-131/12, in *Dejure*; C. giust. UE, sez. III, 11 dicembre 2019, C-708/18, in *Dejure*).

Sul punto, parte autorevole della dottrina *giusfilosofica* ha enucleato la teoria del “**test di proporzionalità**” in tre passaggi: “idoneità”, “necessità”, “proporzionalità o bilanciamento in senso stretto” [Pino 2011, 204 ss.], spiegando che la **proporzionalità** e il **bilanciamento** sono ambedue tecniche del giudizio di **ragionevolezza** ([Corte cost. 19 dicembre 1991, n. 467](#), in *Giur. cost.*, 1991, 6; [Corte cost. 22 dicembre 1988, n. 1130](#), in *Foro it.*, 1990, I, 67), e che quest'ultimo è «parte interna, (...) fase del più ampio *test* di proporzionalità».

Percorrendo il filo di questo ragionamento si tratta di verificare se: **1)** il *contact tracing* risulta “idoneo” a tutelare la salute della collettività sulla base di un giudizio (reso in negativo) di “palese non idoneità”; **2)** è una misura “necessaria” in termini di minore invasività tra quelle disponibili (ci si riferisce alle attuali restrizioni alla libertà personale e alle sue molteplici modalità di manifestazione, dalla libertà di circolazione, di associazione e riunione, etc.), il che ne implica obbligatoriamente la comparazione; **3)** è in grado di assicurare la piena tutela, generale, del diritto alla salute, il che presuppone uno spostamento del raggio di valutazione sul peso dell'obiettivo, il quale deve trovare massima realizzazione nella riduzione del diritto alla tutela dei dati, ovvero, quest'ultima, in una prospettiva rovesciata, non deve risultare eccessiva per il raggiungimento del massimo grado di tutela della salute collettiva.

A noi pare che il tracciamento digitale trovi un ostacolo negli ultimi due passaggi ora descritti. Nel bilanciamento con gli altri diritti fondamentali sopra menzionati, esso non si configura come misura meno invasiva, perché dà luogo ad un controllo della sfera d'azione della persona non meno forte, nella sostanza, di altre limitazioni della libertà personale. In secondo luogo, non è certo che, così facendo, si riesca effettivamente a dare massima copertura al bene pubblico della salute anzitutto perché esulano dal raggio d'azione del controllo i portatori cd. sani del *virus*, che restano il più pericoloso veicolo di trasmissione. Inoltre, la modalità di funzionamento dell'applicazione Immuni, con *bluetooth*, alla distanza di intervento di un metro, se consente di individuare coloro che

L'hanno scaricata sul proprio *smartphone* tramite codici identificativi, affida ad algoritmi il calcolo della vicinanza di ogni contatto e il relativo tempo di esposizione al virus, generando, come prima funzione, una lista di presunti contagiati che non è detto che contraggano il virus, così come non è detto che tutti i presunti contagiati abbiano scaricato l'applicazione. Difatti è probabile che tra i contatti dell'ammalato risultino contagiate persone che non sono in possesso dell'app, le quali continuerebbero a favorire la diffusione della malattia. Il rischio, dunque, può essere duplice, di non riuscire a contenere l'epidemia nazionale e di mettere in moto meccanismi di intelligenza artificiale, da un lato, non necessari e sproporzionati, dall'altro, inefficaci.

Va detto che l'applicazione in questione sarebbe stata selezionata a seguito del parere reso dal Comitato dei Garanti europei (e redatto dal Garante italiano)

([https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-](https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9316030)

[display/docweb/9316030](https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9316030)), **secondo il quale la logica *bluetooth* soddisfa criteri di maggiore selettività e dunque può avere minore impatto sulla *privacy* perché basata su meccanismi volontari di adesione e sulla trasparenza del sistema di funzionamento dell'app, quest'ultima dovuta al rilascio del codice sorgente di sviluppo con licenza “open source” che ne garantirebbe pubblica accessibilità. Ciò può contribuire a fugare i nostri dubbi, almeno in parte, per adesso, e del tutto, forse, non appena avremo certezza che l'applicazione di tracciabilità sarà stata predisposta in adeguamento delle linee guida in materia di tracciamento dei contatti e di geolocalizzazione adottate dall'Organo di controllo europeo il 21 aprile scorso.**

Su queste ci soffermiamo brevemente nel tentativo di fare un po' di luce sulle caratteristiche del funzionamento del *contact tracking*, ma non prima di aver detto, per chiudere il cerchio del vaglio di proporzionalità, che la sua implementazione nella fase 2 dell'epidemia, ormai alle porte, deve avvenire, opportunamente, in costanza delle limitazioni delle altre libertà fondamentali già in vigore.

In questa prospettiva può ritenersi accettabile una **compressione della tutela del dato personale** per effetto di un'attività di tracciamento digitale, nei limiti in cui venga considerata **relativamente necessaria** all'esito di una ponderazione con le odierne restrizioni ai diversi altri diritti della persona. Nella logica del giudizio di proporzionalità significa che la soddisfazione di una tutela piena del bene primario della salute pubblica può essere garantita *anche* dalla limitazione del dato personale, nel

senso, cioè, che la riduzione delle sue forme di tutela non può essere esclusiva ma deve essere temperata con esigenze altrettanto fondamentali della persona.

La seconda ragione sottesa al giudizio relativistico ha carattere operativo ma è tutt'altro che secondaria: il tracciamento digitale raccoglierà una mole di informazioni tale da chiedersi se l'apparato sanitario sarà pronto a fornire una adeguata risposta attraverso la possibilità di effettuare assistenza a domicilio per la somministrazione di tamponi o altri *test* sierologici comunque efficaci, così come di supportare i malati con le relative cure, al fine di dare respiro alle strutture ospedaliere che, fra l'altro, devono garantire la salute dei singoli per motivi anche diversi dal Coronavirus. Per non parlare, poi, della disponibilità dell'uso delle mascherine protettive, rilievo affatto banale vista la perdurante carenza sin dall'inizio della diffusione dell'infezione. In altre parole, occorre un approccio integrato di interventi per la prevenzione della trasmissibilità della malattia, la cui predisposizione, nell'immediato, deve essere accelerata, non potendosi ritenere che sia meno impellente dell'“incorporazione” di un'app. Diversamente qualunque tecnologia d'avanguardia resterà una goccia d'olio in un mare d'acqua.

Quanto, infine, ai tempi successivi alla fase 2, sarà senza dubbio necessario sottoporre a **ri-valutazione** di proporzionalità il *contact tracing* per decidere della sua applicabilità in termini di ragionevolezza, del tutto compatibilmente, del resto, con l'evoluzione del Coronavirus. Ci si riferisce soprattutto al momento in cui si assisterà alla ripresa di tutte le attività lavorative e sociali con il presumibile, pressoché totale, allentamento delle attuali restrizioni, sempre che non arrivi prima il vaccino oppure mutazioni genetiche che ne diminuiscano l'aggressività.

5. Rilievi sul tracciamento dei contatti con riferimento alle Linee-guida dell'Edpb (European Data Protection Board) del 21 aprile 2020.

Tornando al funzionamento del *contact tracing* e in generale alle sue peculiarità tecniche, ci si attende che l'app Immuni (o qualsiasi altro modello che il Governo decidesse di implementare) venga approvata in via definitiva sul piano legislativo conformemente alle Linee-guida 4/2020 “sull'uso dei dati di localizzazione e degli strumenti per il tracciamento dei contatti nel contesto dell'emergenza legata al COVID-19, adottate il 21 aprile 2020 dal Comitato europeo dei Garanti (<https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9322516>).

Nel documento si sottolinea, sotto il profilo dell'“analisi giuridica generale” (§ 3.1., 6 ss.) che «il monitoraggio sistematico e su larga scala dell'ubicazione e/o dei contatti tra persone fisiche costituisce una grave interferenza nella vita privata (...)» che “può essere legittimata solo facendo affidamento su un'adozione volontaria degli utenti” e che “le persone che non intendono o non possono utilizzare tali applicazioni non dovrebbero subire alcun pregiudizio». Inoltre si precisa che «tali app non possano sostituire, ma solo supportare, il tracciamento manuale dei contatti effettuato da personale sanitario pubblico qualificato».

In secondo luogo, deve essere garantito il rispetto del “principio di responsabilizzazione”, relativamente al quale si dispone «le autorità sanitarie nazionali possano essere i titolari di tale trattamento» sebbene non si debba escludere la configurazione di “altri titolari del trattamento” per il tracciamento dei contatti purché «si proceda a definirli con chiarezza e fin dall'inizio nell'ambito dei rispettivi ruoli e responsabilità, sul presupposto, imprescindibile, che di ciò sia data adeguata informazione a tutti gli utenti».

Il Comitato non omette di rilevare «la possibilità del verificarsi di falsi positivi». Evenienza, questa, in cui “è indispensabile poter effettuare **correzioni dei dati** e/o dei risultati delle analisi successive», ciò in ragione «del forte impatto che può avere sui singoli individui l'identificazione per rischio di infezione e il conseguente obbligo di autoisolamento fino a negativizzazione del test». Pertanto sottolinea l'importanza che «il trattamento e la conservazione dei dati» siano «configurati in modo da permettere tecnicamente di apportare le correzioni suddette», a tale riguardo specificando **che il funzionamento degli algoritmi dovrebbe svolgersi «sotto la stretta sorveglianza di personale qualificato al fine di limitare il verificarsi di falsi positivi e negativi».**

Quanto alle modalità di esecuzione della tracciabilità dei contatti, viene considerato di prioritaria importanza il principio della limitazione delle finalità, a norma del quale «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)». Sicché, una volta individuate in modo predeterminato le finalità, sarà anche possibile garantire che «l'uso dei dati personali sia adeguato, necessario e proporzionato».

In questa ottica l'Organo di controllo europeo auspica «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”. Successivamente detta alcune raccomandazioni relative alla individuazione di precisi requisiti di carattere funzionale che le app devono possedere (§ 3.2, 8 s.).

Le informazioni da raccogliere devono risultare necessarie (non si reputano necessari, per esempio, dati anagrafici, identificativi di comunicazione, voci di directory del dispositivo, messaggi, registrazioni di chiamate, dati relativi all'ubicazione, identificativi del dispositivo, ecc.). Specificatamente la raccolta deve essere effettuata utilizzando «identificatori univoci e pseudonimi, generati dall'app e specifici di tale app», che devono «essere rinnovati regolarmente» per “limitare il rischio di identificazione e di localizzazione fisica delle persone». Per questo motivo il Comitato suggerisce l'attivazione di modalità corrette per il trattamento dei dati sin dalla fase di progettazione e per impostazione predefinita (*by design* e *by default*) conformemente al principio di minimizzazione del trattamento.

L'Edpb non vieta il trasferimento delle informazioni in un database centralizzato purché «siano in vigore adeguate misure di sicurezza» e comunque andrebbe previsto nella fase di progettazione e ponderato con l'approccio decentrato, nell'ottica di poter valutare l'impatto di entrambi sui diritti delle persone. Fermo restando – si sottolinea – che «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 dell'utente stesso». In questa ottica le sole tecniche da utilizzare validamente sono quelle «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». Difatti la modalità di segnalazione nell'app di utenti infetti da Covid-19 deve svolgersi secondo procedure precise, quali, ad esempio, l'impiego di un codice monouso correlato a una identità pseudonima della persona infetta e collegato a un laboratorio o a un operatore sanitario.

Per quanto riguarda, nel nostro caso, l'app Immuni – e si conclude – non dovrebbero esserci ostacoli nel recepire gli orientamenti ora descritti, alcuni dei quali sembrano essere già stati accolti. Ci si riferisce al criterio della adesione volontaria, alla pubblicità del codice sorgente, all'utilizzo di codici identificativi nel rispetto del criterio di

minimizzazione, e naturalmente alla specificazione delle finalità di contrasto e contenimento del contagio epidemico, e della durata dei trattamenti legati alla tracciabilità limitatamente a quello che sarà il tempo di vita del Covid-19.

Il vero nodo della questione, al momento, consiste invece nella scelta dell'approccio, **centralizzato** o **localizzato**. Non risulta chiaro, cioè, se le informazioni utili a rendere identificabili gli utilizzatori vengano raccolte dal server dello *smartphone*, oppure da un database centralizzato, e in questo caso non si sa per quali -ulteriori- finalità oltre quella di elaborare un profilo di rischio per ogni persona entrata in contatto con l'utilizzatore risultato positivo e di inviargli un **alert**, cioè un segnale di notifica per informarlo del pericolo di aver contratto il virus e quindi della necessità di sottoporsi ad autoisolamento e ai relativi controlli sanitari. Sarebbe certamente più coerente con la filosofia della protezione dei dati lasciare al singolo il controllo delle proprie informazioni consentendo la “conservazione locale” dei dati su ciascun dispositivo ma pare che a questo sia *Apple* che *Google play* stiano già lavorando, vedremo con quale esito.

6. Riferimenti bibliografici.

T. Epidiendo, *Il diritto nello “stato di eccezione” ai tempi dell'epidemia da Coronavirus*, in www.giustiziainsieme.it, 30 marzo 2020.

L. Cuocolo, *Presentazione*, in Id., (a cura di), *I diritti costituzionali di fronte all'emergenza Covid-19: una prospettiva comparata*, 5-7, in Ffederalismi.it; nonché, ivi, *I diritti costituzionali di fronte all'emergenza Covid-19: la reazione italiana*, 12 ss.; sempre ivi per la visione di altri *Report*.

C. Caruso, *La pandemia aggredisce anche il diritto?*, Intervista a Corrado Caruso, Giorgio Lattanzi, Gabriella Luccioli e Massimo Luciani, in <https://giustiziainsieme.it> del 2 aprile 2020.

In tema di diritto alla protezione dei dati personali: R. Lattanzi, “*Diritto alla protezione dei dati di carattere personale*”: *Appunti di viaggio*, in AA.VV., *Diritto alla privacy e trattamento automatizzato dei dati fra diritto civile, diritto penale e diritto internazionale ed europeo*, in *I quaderni europei*, aprile 2014, 63, 10 ss.

Sui criteri di proporzionalità e ragionevolezza nell'interpretazione dei giudici costituzionali, si veda L. Mengoni, *Il diritto costituzionale come diritto per principi*, in

Ars interpretandi 1996, 95 ss. Nell'ambito della dottrina giusfilosofica: G. Pino, *Diritti e interpretazione*, Bologna, 2011, 204 ss., in particolare, 205, nt. 13, per gli opportuni riferimenti bibliografici. L'A. è tornato sul tema in scritti più recenti: *Diritti fondamentali e principio di proporzionalità*, in *Ragion pratica*, 2014, vol. XLIII, 541 ss.; *Proporzionalità, diritti, democrazia*, in *Diritto e società*, n. 3/2014, 597 ss.; e da ultimo, ampiamente, nel volume *Il costituzionalismo dei diritti*, Bologna, 2017, 42-45 e 143-163. Per la dottrina giuslavoristica, in considerazione dell'ampiezza e complessità del tema, sia consentito il rinvio, per tutti, al volume di G. Fontana, *Dall'inderogabilità alla ragionevolezza*, Torino, 2010.

Per un primo commento al Protocollo del 14 marzo 2020, si v. E. Dagnino, *La tutela della privacy ai tempi del coronavirus: profili giuslavoristici*, in *Giustiziacivile.com*, 17 marzo 2020. Sul dibattito in tema di salute e sicurezza nei luoghi di lavoro appena sorto in relazione alla natura del rischio da Covid-19 e alla correlata opportunità di aggiornare la valutazione dei rischi e il relativo documento, si rinvia a P. Pascucci, *Coronavirus e sicurezza sul lavoro, tra "raccomandazioni" e protocolli. Verso una nuova dimensione del sistema di prevenzione aziendale?*, in *Dir. sic. lav*, 2, 2019, 98 ss.; Id., *Sistema di prevenzione aziendale, emergenza coronavirus ed effettività*, in *Giustiziacivile.com*, 2020, 17 marzo 2020; Id., *Ancora su coronavirus e sicurezza sul lavoro: novità e conferme nello ius superveniens del [d.P.C.M. 22 marzo 2020](#) e soprattutto del [d.l. n. 19/2020](#)*, in *Dir. sic. lav.*, 2020, n. 1, 117 ss. *Contra*, R. Guariniello, *La sicurezza sul lavoro al tempo del coronavirus*, Mialno, 2020, 10 ss.; G. Natullo, *Covid-19 e sicurezza su lavoro: nuovi rischi, vecchie regole?* in *WP C.S.D.L.E. "Massimo D'Antona".IT*, n. 413, 2020; A. Ingraio, *C'è il COVID, ma non adeguati dispositivi di protezione: sciopero o mi astengo?*, in *Giustiziacivile.com*, 18 marzo 2020; R. Dubini, *COVID-19: sulla valutazione dei rischi da esposizione ad agenti biologici*, in *Punto sicuro*, 2 marzo 2020; M. Gallo, *Coronavirus, obblighi del datore per tutelare i lavoratori a contatto con il pubblico*, in *Guida lav.*, 10, 2020. Si sofferma sulla sperimentazione di test sierologici per proteggere la salute in azienda, M.T. Carinci, *Back to work al tempo del Coronavirus e obbligo di sicurezza del datore di lavoro. I test sierologici rapidi*, in *Adapt Labour Studies e-Book series*, n. 3, 2020; F. Bacchini, *Controlli sanitari sui lavoratori al tempo del COVID-19*, in *Giustiziacivile.com*, 18 marzo 2020.

