Covid-19 e Protezione dei dati personali

di Giuliana Amore (*)

Sommario: 1. Premessa. – 2. La c.d. *app* "Immuni" come misura emergenziale. – 3. (*Segue*). Il problema della liceità dell'*app* "Immuni": quale base giuridica. – 4. (*Segue*). Le garanzie per l'interessato: limitazione della finalità, minimizzazione e anonimizzazione dei dati personali.

1. Premessa

Com'è noto, (anche) i principi in materia di protezione dei dati contenuti nella c.d. *data protection law*, ossia nel Reg. UE n. 679 del 2016, sono messi a dura prova dal *Covid-19* e sono chiamati a svolgere un ruolo fondamentale: per rendersene conto, è sufficiente guardare l'imponente stratificazione, occorsa negli ultimi mesi e in costante aggiornamento, di disposizioni emanate in relazione all'emergenza scaturita dalla diffusione dell'epidemia *Covid-19*, a partire dall'inizio dell'anno e aventi, per quel che rileva ai nostri fini, un impatto sul trattamento di dati personali e, conseguentemente, sul diritto alla loro protezione (1).

(*) Contributo pubblicato previo parere favorevole formulato da un componente del *Comitato per la valutazione scientifica*.

(1) Di particolare rilievo, il d.l. 9 marzo 2020, n. 14, art. 14, alla cui stregua «fino al termine dello stato di emergenza deliberato dal Consiglio dei ministri in data 31 gennaio 2020, per motivi di interesse pubblico nel settore della sanità pubblica e, in particolare, per garantire la protezione dall'emergenza sanitaria a carattere transfrontaliero determinata dalla diffusione del *Covid-19* mediante adeguate misure di profilassi, nonché per assicurare la diagnosi e l'assistenza sanitaria dei contagiati ovvero la gestione emergenziale del Servizio sanitario nazionale, nel rispetto dell'art. 9, paragrafo 2, lettere *g*), *h*) e *i*), e dell'art. 10 del Regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 […] possono effettuare trattamenti, *ivi* inclusa la comunicazione tra loro, dei dati personali, anche relativi agli artt. 9 e 10 del Regolamento UE 2016/679, che risultino necessari all'espletamento delle funzioni attribuitegli nell'àmbito dell'emergenza determinata dal diffondersi del *Covid-19* […] I trattamenti di dati personali di cui ai commi 1 e 2 sono effettuati nel rispetto dei principi di cui all'art. 5 del citato Regolamento UE 2016/679, adottando misure appropriate a tutela dei diritti e delle libertà degli interessati»; il d.l. 30 aprile 2020 n. 28, art. 6, secondo il quale «al solo fine 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'àmbito delle misure di sanità pubblica legate all'emergenza *Covid-19*, 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 Ministero della salute, all'esito di una valutazione di impatto, costantemente aggiornata, effettuata ai sensi dell'art. 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'art. 36, paragrafo 5, del medesimo Regolamento UE 2016/679 e dell'art. 2-*quinquiesdecies* del Codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196, assicurando, in particolare, che: *a*) gli utenti ricevano, prima dell'attivazione dell'applicazione, ai sensi degli artt. 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; 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; è esclusa in ogni caso la geolocalizzazione dei singoli utenti; […] *d*) siano garantite su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento nonché misure adeguate ad evitare il rischio di reidentificazione degli interessati cui si riferiscono i dati pseudonimizzati oggetto di trattamento; […] 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'àmbito delle misure di cui al presente comma; i dati sono cancellati in modo automatico alla scadenza del termine. […] 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. Il d.l. 10 maggio 2020, n. 30, all'art. 1 dispone che in considerazione della necessità di disporre con urgenza di studi epidemiologici e statistiche affidabili e complete sullo stato immunitario della popolazione, indispensabili per garantire la protezione dall'emergenza sanitaria in atto, ai sensi dell'art. 9, paragrafo 2, lettere *g*) e *j*), e dell'art. 89 del Regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, nonché dell'art. 2-*sexies*, comma 2, lettera *cc*) del decreto legislativo 30 giugno 2003, n. 196, è autorizzato il trattamento dei dati personali, anche genetici e relativi alla salute, per fini statistici e di studi scientifici svolti nell'interesse pubblico nel settore della sanità pubblica, nell'àmbito di un'indagine di "siero-prevalenza" condotta congiuntamente dai competenti Uffici del Ministero della salute e dall'Istituto nazionale di statistica (ISTAT), in qualità di titolari del trattamento e ognuno per i profili di propria competenza, secondo le modalità individuate dal pre-

Tra le misure proposte e già adottate per far fronte all'emergenza derivante dalla pandemia, vi sono quelle basate sulla raccolta e sul tracciamento di dati personali sanitari per il controllo e il contenimento del *virus*: ci si intende in particolare riferire alla c.d. *app* "Immuni".

Trattasi di una misura che, *prima facie*, sembrerebbe implicare un controllo invasivo nella vita delle persone: il monitoraggio sull'andamento del *virus* si potrebbe tradurre, di fatto, in un conseguente monitoraggio della persona stessa ed emblematica al riguardo è l'esperienza cinese, il cui Governo ha sviluppato insieme alle Autorità sanitarie, un'*app* per tracciare le persone infette o potenzialmente tali. In altri termini, ci troviamo di fronte ad un sistema che, sebbene finalizzato al contenimento del rischio, potrebbe essere idoneo a raccogliere numerose informazioni su ciascun cittadino, a partire dai dati sanitari (2), che, com'è noto, rappresentano dati particolarmente "sensibili" alla luce del Reg. UE n. 679 del 2016 (c.d. GDPR).

Ci si chiede, pertanto, se una tale situazione di emergenza sanitaria possa effettivamente giustificare misure atte ad annullare (o quasi) la tutela della *privacy*, attraverso la predisposizione di *app* o simili strumenti che invadano la sfera personale dell'individuo: verifica che non può farsi in astratto, bensì caso per caso, cioè in relazione allo specifico sistema di tracciamento o di monitoraggio in concreto adottato. E se da un lato le tecnologie digitali possono senz'altro essere elementi chiave nella lotta al *Covid-19*, dall'altro lato occorre tuttavia proteggersi dal rischio di effetti che potrebbero rivelarsi irreversibili, nel senso che è indispensabile garantire che ogni misura adottata in queste circostanze eccezionali sia necessaria, limitata nel tempo, di portata minima e soggetta a un riesame periodico ed effettivo: bisogna cioè contemperare le esigenze di gestione dell'emergenza sanitaria in atto con quella afferente alla salvaguardia della riservatezza degli interessati (3).

È altrettanto noto come, a fronte dell'emergenza, sia in atto uno sforzo congiunto per combattere il diffondersi di una malattia infettiva, ancora pressoché sconosciuta, che mette in pericolo la salute dei cittadini di tutto il mondo: allo stesso tempo, sia lo *European Data Protection Board* (*EDPB*) sia il Garante per la protezione dei dati personali avvertono, però, che le misure assunte dovranno comunque essere immediatamente revocabili al termine

AS

sente articolo e dal protocollo approvato dal Comitato Tecnico Scientifico di cui all'art. 2 dell'ordinanza del Capo del Dipartimento della protezione civile 3 febbraio 2020, n. 630, nonché nel rispetto delle pertinenti Regole deontologiche allegate al medesimo decreto legislativo n. 196/2003 […] Il trattamento dei campioni e dei relativi dati è effettuato per esclusive finalità di ricerca scientifica sul SARS-COV-2 individuate dal protocollo di cui al comma 1, nel rispetto delle prescrizioni del Garante per la protezione dei dati personali individuate nel provvedimento del 5 giugno 2019 e successive modificazioni. Il titolare del trattamento dei dati raccolti nella banca biologica è il Ministero della salute e l'accesso ai dati da parte di altri soggetti, per le predette finalità di ricerca, è consentito esclusivamente nell'àmbito di progetti di ricerca congiunti con il medesimo Ministero».

(2) Trattasi dei dati relativi alla salute, fisica e mentale. Il Considerando n. 35 elenca esemplificativamente alcuni dati sanitari, come «le informazioni risultanti da esami e controlli effettuati su una parte del corpo o una sostanza organica, compresi i dati genetici e i campioni biologici; qualsiasi informazione riguardante, ad esempio, una malattia, una disabilità, il rischio di malattie, l'anamnesi medica, i trattamenti clinici o lo stato fisiologico o biomedico dell'interessato, indipendentemente dalla fonte, quale ad esempio un medico o un operatore sanitario, un ospedale, un dispositivo medico o un *test* diagnostico in vitro». Sul punto, cfr. L. Bolognini – E. Pelino – C. Bistolfi, *Il Regolamento* Privacy *europeo*, Milano 2016, p. 71.

(3) Con precipuo riferimento al contesto lavorativo, il Garante ha specificato, in particolare, che, nell'àmbito del sistema di prevenzione e sicurezza sui luoghi di lavoro o di protocolli di sicurezza anti-contagio, il datore di lavoro può richiedere ai propri dipendenti di effettuare *test* sierologici solo se disposto dal medico competente o da altro professionista sanitario in base alle norme relative all'emergenza epidemiologica. Solo il medico del lavoro, infatti, nell'àmbito della sorveglianza sanitaria, può stabilire la necessità di particolari esami clinici e biologici. E sempre il medico competente può suggerire l'adozione di mezzi diagnostici, quando li ritenga utili al fine del contenimento della diffusione del *virus*, nel rispetto delle indicazioni fornite dalle autorità sanitarie, anche riguardo alla loro affidabilità e appropriatezza. Con riguardo, poi, alla tutela dei luoghi di lavoro rispetto ai visitatori e alla somministrazione di veri e propri questionari sui comportamenti e sui dati sanitari di tali soggetti, il Garante *Privacy* ha precisato che il compito relativo all'accertamento e alla raccolta di informazioni relative a potenziali situazioni di contagio – presenza di sintomi influenzali, spostamenti in luoghi considerati a rischio, contatto con persone dei cc.dd. "focolai", ecc. – spetta esclusivamente agli organi competenti, rinvenibili negli operatori sanitari nonché nella Protezione Civile. Viene, pertanto, espressamente vietato ai soggetti privati, tra cui anche i Datori di Lavoro, di procedere ad autonome indagini così come a specifiche richieste di informazioni. Secondo il Garante, tale pratica sarebbe eccessiva ed ingiustificata. L'Autorità precisa anche che le informazioni relative alla diagnosi o all'anamnesi familiare del lavoratore non possono essere trattate dal datore di lavoro (ad esempio, mediante la consultazione dei referti o degli esiti degli esami). Per converso, il datore di lavoro potrà comunicare la presenza di un caso di infezione di *Covid-19* ai dipendenti e collaboratori senza comunicare informazioni che non siano necessarie a tale scopo e adottando misure di protezione efficaci; in caso di divulgazione del nome, bisognerà informare preventivamente il soggetto interessato nel rispetto della sua dignità ed integrità. Il Garante ha chiarito infine che la partecipazione agli *screening* sierologici promossi dai Dipartimenti di prevenzione regionali nei confronti di particolari categorie di lavoratori a rischio di contagio, come operatori sanitari e forze dell'ordine, può avvenire solo su base volontaria. I risultati possono essere utilizzati dalla struttura sanitaria che ha effettuato il *test* per finalità di diagnosi e cura dell'interessato e per disporre le misure di contenimento epidemiologico previste dalla normativa d'urgenza in vigore (es. isolamento domiciliare).

del periodo di emergenza, in modo da evitare una abnorme compressione dei diritti fondamentali degli interessati. Sebbene la finalità sia rappresentata dalla gestione dell'emergenza e dal contenimento del contagio in modo da tutelare la salute dell'intera popolazione, numerosi sono i dubbi in merito alle modalità e alla necessità del trattamento, con metodi sistematici e su larga scala, dei dati sanitari e/o di altri dati dei soggetti interessati. Il nostro Paese, dunque, analogamente ad altri Stati europei, ha affrontato e risolto positivamente la questione dell'assunzione di misure a tutela del diritto alla salute, che potrebbero comportare il trattamento di dati personali "particolari" o sensibili su larga scala dei soggetti interessati, ma anche la profilazione (4) derivante dalla combinazione di questi dati: da qui, la necessità di verificare se si tratti o meno di soluzioni *legittime*, eccessivamente pervasive e poco efficaci, soprattutto se non accompagnate dalla fornitura di un adeguato numero di dispositivi di protezione per sanitari e per cittadini, oltreché dall'effettuazione di tamponi per la rilevazione del *Covid-19*.

2. La c.d. *app* "Immuni" come misura emergenziale

Il Governo ha notoriamente optato per la c.d. app "Immuni" (5) per la gestione del *contact tracing* (o tracciamento dei contatti) nella fase 2 e 3 dell'emergenza *Coronavirus* (6). Essa è stata sostanzialmente sviluppata dalla società italiana *Bending Spoons* e trova la propria *ratio* ufficiale principalmente in due considerazioni: la capacità di contribuire tempestivamente all'azione di contrasto del *virus* e la conformità al modello europeo delineato dal Consorzio PEPP-PT (7). Il problema è quello di indagare la liceità di tale strumento e, in caso di esito positivo di siffatta valutazione, di individuare le garanzie per il rispetto della *privacy*.

Propedeutica per la soluzione di entrambe le questioni è una sia pur breve disamina delle caratteristiche dell'*app* "Immuni". Trattasi di un'*app* di tracciamento di prossimità, in quanto permette scambi di dati tra dispositivi che sono tra loro vicini e che hanno il *bluetooth* attivato. A ogni dispositivo è assegnato un ID temporaneo e mutevole: se un individuo nel cui *smartphone* sia presente "Immuni" scopre di essere positivo al *coronavirus*, gli viene fornito un codice con il quale può scaricare su un *server* l'elenco degli ID degli *smartphone* che hanno a loro volta installato e attivato "Immuni" e con i quali è entrato in contatto nei giorni precedenti.

A tutti questi contatti viene inviata una notifica del rischio di contagio, sempre tramite la *app*. Questa risulta composta da due parti, una dedicata al *contact tracing* vero e proprio (via *Bluetooth*) e l'altra destinata ad ospitare una sorta di "diario clinico", in cui l'utente possa annotare progressivamente i dati relativi alle proprie condizioni di salute, come la presenza di sintomi compatibili con il *virus*. I cellulari conservano in memoria i dati di altri cellulari con cui sono entrati in contatto, in forma di codici anonimi crittografati. Associati a questi codici ci sono dei metadati (quali la durata dell'*incontro* tra i dispositivi o la forza del segnale percepito) che entrano in gioco nella valutazione – fatta

(4) Com'è noto, l'art. 4 del *GDPR* definisce la profilazione come «qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica». Quindi, per stabilire se si è in presenza di profilazione è opportuno verificare se le persone fisiche siano tracciate su *internet*, compreso l'eventuale ricorso successivo a tecniche di trattamento dei dati personali che consistono nella *profilazione* della persona fisica, in particolare per adottare decisioni che la riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali. Dunque, l'attività di profilazione si compone di: trattamento automatizzato; svolgimento su dati personali; finalità valutativa degli aspetti personali di una persona fisica. Sussiste una specifica disciplina della profilazione proprio in àmbito sanitario: l'art. 22, par. 4, del *GDPR*, come principio generale, vieta la profilazione dei dati sanitari. Pertanto, anche nei casi in cui il divieto generale di profilazione viene derogato, tale deroga non si applica all'acquisizione dei dati sanitari. Infatti, questi, essendo classificati come dati personali particolari *ex* art. 9 *GDPR*, necessitano di una particolare tutela. Il divieto di profilazione può tuttavia essere derogato in specifici casi: in particolare, l'attività di profilazione di dati sanitari potrà avvenire eccezionalmente nell'ipotesi in cui c'è un consenso esplicito dell'interessato; oppure va perseguito un interesse pubblico rilevante nell'àmbito della sanità pubblica; il titolare (o responsabile) abbia adottato idonee ed adeguate misure di sicurezza per tutelare i diritti, le libertà e i legittimi interessi del paziente.

(5) Attualmente in fase di sperimentazione in alcune Regioni e, a partire dal 15 giugno, attiva in tutta Italia.

(6) Erano state individuate due sole soluzioni tecnologiche, ritenute teoricamente valide per essere sviluppate e testate a scopo di implementazione nell'attuale situazione emergenziale: "Immuni" e "*CovidApp*". All'esito della sua analisi comparativa, la *task force* è giunta alla conclusione per cui "Immuni" utilizzerebbe la tecnologia sviluppata dal Consorzio Progetto Europeo PEPP-PT, promettendo quindi maggiori garanzie di interoperabilità e anonimizzazione dei dati personali. Tale soluzione inoltre è stata ritenuta ad uno stadio di sviluppo più avanzato della soluzione *CovidApp*. Sull'*app* "Immuni", cfr. in particolare l'intervista su *www.qds.it* a Salvatore Sanfilippo, noto programmatore informatico, ideatore di "Redis".

(7) In effetti tale modello è stato adottato soltanto in parte dall'*app*; poi l'*app* ha cambiato modello adottando quello di Apple-Google, più decentralizzato.

direttamente sul singolo *device* – del rischio contagio. Allorché uno dei soggetti che ha scaricato l'*app* risulti positivo al *virus*, gli operatori sanitari gli forniscono un codice di autorizzazione con il quale questi può scaricare su un *server* ministeriale il proprio codice anonimo, secondo un modello decentralizzato. I cellulari con l'*app* prendono dal *server* i codici dei contagiati (8) e se l'*app* riconosce tra i codici nella propria memoria un codice di un contagiato, visualizza la notifica all'utente. La trasmissione dei dati risulta cifrata e firmata digitalmente per garantire la massima sicurezza e riservatezza in questa fase di "uscita" del dato dallo *smartphone* del singolo utente.

L'intera architettura del sistema scelto dal governo italiano per raccogliere dati utili a ricostruire i contagi da corona*virus* poggia su un'applicazione che registra i dati, li condivide con il *server* centrale e interroga gli archivi per verificare contatti a rischio. L'*app* associa ogni telefono su cui viene installata a un codice casuale anonimo. Una volta scaricata la piattaforma e attivato il sistema di notifica, lo *smartphone* comincia a scambiare via *Bluetooth* il proprio codice (anonimo e casuale) con gli altri *smartphone* che si trovano nelle vicinanze e che hanno scaricato l'*app* di *contact tracing*. Se un cittadino risulta positivo al *Coronavirus* può inserire nell'*app* un codice di verifica consegnato con il *test*. A quel punto l'*app* comunica a un *server* centrale (9) la zona di provenienza, la Provincia di residenza e le informazioni epidemiologiche del soggetto positivo al *coronavirus*. Solo dopo questi passaggi, coloro che negli ultimi giorni sono stati in contatto per più di qualche minuto con il contagiato vengono avvertiti con un *alert*, ma non sembra possibile risalire né alla persona, né al luogo o all'orario dell'incontro.

La *app*, una volta ricevuta l'indicazione che un soggetto è risultato positivo, invia una notifica a tutti gli ID che sono stati "a contatto" con lui nelle precedenti due settimane; il soggetto che riceve la notifica viene semplicemente messo nelle condizioni di conoscere il rischio contagio e starà a lui adottare volontariamente misure di maggior precauzione (magari "raccomandate" dalla *app* in fase di notifica). Aperta la notifica, si può conoscere solo la data del contatto, mentre spetta poi alle autorità sanitarie su base regionale il compito di dare consigli su come comportarsi. L'*app* può essere disattivata in ogni momento e i dati dei singoli incontri risultano conservati sui dispositivi personali, e non su un *server* centrale (10).

È stata fermamente esclusa l'ammissibilità di forme di imposizione (sia pur di fatto) dell'*app*, contrariamente all'orientamento e alla proposta che la commissione tecnico-scientifica del governo sul *Coronavirus* stava per formalizzare al fine di rendere l'*app* quasi obbligatoria: al riguardo, si era ipotizzato di renderla *condicio sine qua non* per la fruizione di vantaggi (quali la mobilità nella fase 2), abbinandola all'autocertificazione. La soluzione adottata si palesa rispettosa delle raccomandazioni dello *European Data Protection Board* (*EDPB*) e del Garante per la protezione dei dati personali, che vigilano sull'osservanza dei profili giuridici dell'applicativo di *contact tracing* e che hanno caldamente sconsigliato sia l'installazione obbligatoria, sia l'attuazione di forme di incentivo che graduino o limitino, financo escludano, l'accesso dei cittadini a servizi altrimenti fruibili secondo principi di parità di trattamento o che vincolino l'esercizio di diritti di libertà all'adozione dell'*app*: obblighi, che dichiarati o mascherati da incentivi, rappresenterebbero senz'altro una forma di invadenza nella sfera privata implicante dubbi di costituzionalità ma che, se non previsti, come dimostrato dall'evidenza e dai dati quotidiani, determinano inevitabilmente un depotenziamento dell'efficacia dell'*app* a scapito della protezione di un interesse di rango altrettanto costituzionale (e forse superiore), quello della salute pubblica. Limitandoci agli aspetti strettamente inerenti all'indagine, va osservato come i limiti e gli obblighi imposti al diritto alla *privacy* interferiscano con altri diritti fondamentali e, segnatamente, con il diritto alla salute: tali diritti non hanno prevalenza assoluta l'uno sugli altri, e nemmeno il diritto alla protezione dei dati può far da "tiranno" (11): quest'ultimo, disciplinato specificamente

(8) Nel modello centralizzato i cellulari riceverebbero direttamente dal *server* la eventuale notifica di "soggetto a rischio".

(9) Questo *server* sarebbe un'infrastruttura pubblica italiana, gestita da Sogei, con una piattaforma *software* gestita dal Ministero della Salute.

(10) In sintesi, l'*app* crea un registro dei contatti con cui si "comunica", archiviando tre informazioni per ciascun utente: quale è il dispositivo con il quale si è entrati in contatto, a che distanza e per quanto tempo. Se un soggetto con cui si è entrato in contatto risulterà positivo al *Covid-19* a seguito di un *test*, l'operatore medico autorizzato dal cittadino positivo, attraverso l'identificativo anonimo dello stesso, farà inviare un *input*/messaggio di *alert* per informare gli utenti identificati in modo anonimo che sono entrati in contatto con lui. Per *privacy*, l'*alert*/messaggio ricevuto non contiene l'identificativo della persona risultata positiva al *Covid-19*, ma informa che qualcuno con cui si è stati in contatto, è risultato positivo al nuovo *coronavirus*, con informazioni su come comportarsi di conseguenza.

(11) Nessun diritto fondamentale è protetto in termini asso-

all'art. 8 della Carta europea dei diritti fondamentali dell'Unione europea, rientra nell'alveo dell'art. 52, par. 1 e 3 della Carta medesima (12) e, in quanto tale va, caso per caso, bilanciato rispetto agli altri diritti riconosciuti come fondamentali. Da tale norma sembra possibile evincere l'attribuzione di una specifica preminenza, ricorrendone determinati presupposti tra cui senz'altro le situazioni emergenziali in àmbito sanitario, agli obiettivi di interesse generale, quale la tutela della salute pubblica. Il conflitto tra interesse alla protezione della salute collettiva, contenuto nell'art. 35 della Carta dei diritti fondamentali dell'Unione Europea, e interesse alla protezione dei dati personali *ex* art. 8 Carta UE dovrebbe forse più correttamente risolversi a favore del primo, in nome del quale giustificare un'invasione della sfera privata: ciò, per la sua rilevanza non solo individuale, bensì generale e sociale o per l'appunto «della collettività» (art. 32 Cost.). Si tratta di operare un raffronto e soppesare i benefici e gli obiettivi perseguiti (salute pubblica) che deriverebbero dall'imposizione di sacrifici ad altri diritti e interessi in gioco (protezione dei dati personali), alla luce del principio di "proporzionalità in senso stretto". È questa la questione più delicata, che esige che il legislatore (prima) e l'interprete (dopo) «spalanchi(no) lo sguardo delle *proprie* valutazioni, fino a proiettarsi sull'impatto effettivo» (13) delle misure emergenziali introdotte, bilanciando diritti e interessi in gioco e ricercando la soluzione che più di ogni altra persegua in modo equilibrato la massima espansione di tutti i diritti e i valori coinvolti (14).

3. (*Segue*). Il problema della liceità dell'*app* "Immuni": quale base giuridica

Lo *European Data Protection Board* (*EDPB*), nei mesi scorsi, ha adottato una Dichiarazione formale e una serie di linee guida proprio sull'uso dei dati di localizzazione e degli strumenti per il tracciamento, in merito al trattamento dei dati personali nel contesto dell'epidemia, sottolineando l'importanza di garantire sempre la tutela dei dati personali e delle persone fisiche interessate: ciò, soprattutto al fine di evitare eventuali contagi di ritorno

luti dalla Costituzione, ma – al contrario – è soggetto a limiti per integrarsi con una pluralità di altri diritti e valori, giacché altrimenti si farebbe "tiranno" e porterebbe al totale annientamento di uno o più fattori in gioco: in tal senso, Corte cost. n. 85 del 2013, *supra* citata.

(12) Eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui.

(13) Così, M. Cartabia, *I principi di ragionevolezza e proporzionalità nella giurisprudenza costituzionale italiana*, in *Atti del seminario svoltosi in Roma*, Palazzo della Consulta, 13-14 ottobre 1992, Milano 1994, p. 5 e in *Atti della Conferenza trilaterale delle Corti costituzionali italiana, portoghese e spagnola*, Roma 2013, p. 12.

(14) Com'è noto, nella giurisprudenza costituzionale italiana, il giudizio di bilanciamento dei diritti è conosciuto e praticato da molto tempo, come strumento indispensabile per l'attuazione di una Costituzione pluralista, che accoglie una concezione "dignitaria" dei diritti, distinta da quella c.d. "libertaria": i diritti fondamentali non sono mai affermati in termini assoluti, ma fanno parte di un tessuto costituzionale complesso in cui altri diritti e altri interessi e beni costituzionalmente protetti possono legittimamente limitarne la portata. Nella Costituzione italiana, ogni diritto è sempre predicato assieme al suo limite e, in questo àmbito, il bilanciamento è una tecnica interpretativa e argomentativa che consente il necessario ragionevole contemperamento o proporzionalità di una pluralità di interessi costituzionali concorrenti: emblematica, al riguardo, la recente sentenza sul caso ILVA, n. 85 del 2013, in cui la Corte ha esplicitato il carattere non assolutamente prevalente dei diritti fondamentali, oggetto, piuttosto, di un bilanciamento. Alla interruzione delle attività delle acciaierie ILVA di Taranto, ordinata dal giudice a tutela della salute dei lavoratori e dei cittadini, si è contrapposta l'esigenza di preservare un'attività economica di grande impatto nella società italiana ed europea, soprattutto per l'enorme numero di posti di lavoro messi a rischio dagli effetti irreversibili dello spegnimento dell'alto forno ordinato dal giudice. La Corte si è trovata, dunque, di fronte a due ordini di diritti in conflitto: il diritto alla salute e all'ambiente, da un lato, e diritto al lavoro e all'esercizio delle attività economiche dall'altro. In questo contesto la Corte, con una formulazione particolarmente efficace, ha affermato 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» (sentenza n. 264 del 2012). 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. […]». Sull'argomento, senza alcuna pretesa di completezza data la complessità del tema e la vastità di letteratura in materia, cfr. *ex multis*, R. Bin, *Diritti e argomenti: il bilanciamento degli interessi nella giurisprudenza costituzionale*, Milano 1992; G. Pino, *Diritti umani tra norme, fatti e retorica. Diritti fondamentali e principio di proporzionalità*, in *Ragion pratica* 2014, p. 541 ss.; D.U. Galetta, *Il principio di proporzionalità nella Convenzione europea dei diritti dell'uomo, fra principio di necessarietà e dottrina del margine di apprezzamento statale: riflessioni generali su contenuti e rilevanza effettiva del principio*, in *R. it. d. pubbl. comun.* 1999, p. 743 ss.; C. Sartoretti, *Il diritto alla* privacy *tra sicurezza e principio di proporzionalità: il punto di vista della Corte europea dei diritti dell'uomo*, in *D. pubbl. comp. eur.* 2009, p. 583; A. Sitzia, *I «controlli tecnologici» del datore di lavoro tra necessità e proporzionalità. Chiare indicazioni lavoristiche dalla prima Sezione civile*, in *Nuova g. civ. comm.* 2014, 2, p. 103 ss. Nella letteratura straniera, in particolare, cfr. A. Barak, *Proportionality*, Cambridge 2012, p. 175 ss.; A. Stone Sweet – J. Mathews, *Proportionality Balancing and Global Constitutionalism*, in *47 Columbia Journal of Transnational Law* 2008, p. 73.

una volta allentate le misure di contenimento adottate, nonché per consentire il controllo e l'isolamento di nuovi focolai. In tale documento viene raccomandato il rispetto, anzitutto, del principio di liceità del trattamento conseguente all'adozione delle misure emergenziali, tra le quali si colloca per l'appunto l'*app* "Immuni".

Sul piano ermeneutico, il problema fondamentale è quello di verificare se l'emergenza sanitaria possa rappresentare la base giuridica per legittimare la restrizione della libertà al trattamento dei dati sanitari. Orbene, nel Considerando n. 46 del *GDPR*, si definisce lecito il trattamento svolto per controllare «l'evoluzione di epidemie e la loro diffusione o in casi di emergenze umanitarie», e viene richiamato l'art. 9.2, lett. *i)*, dello stesso *GDPR*, che prevede per l'appunto il trattamento in situazioni di emergenza sanitaria, come quella causata dal *Coronavirus*, e alla cui stregua il trattamento di dati particolari – nella specie, sanitari – è consentito in caso di gravi minacce per la salute e la sicurezza sociale o collettiva, sulla base di un bilanciamento tra diversi diritti costituzionalmente garantiti: il bene della salute collettiva, da un lato e la tutela della riservatezza, dall'altro.

Più precisamente, l'art. 9, dopo aver posto (par. 1) il divieto generale di trattamento dei dati particolari (15), quali quelli «relativi alla salute», ammette il trattamento stesso allorché (tra l'altro) esso sia «necessario per motivi di interesse pubblico nel settore della sanità pubblica», come la protezione da «gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria, dei medicinali e dei dispositivi medici sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato» [art. 9, par. 2, lett. *i*)].

Ma se il trattamento dei dati sanitari appare dunque legittimo alla luce dell'art. 9.2, lett. *i*), *GDPR*, a destare preoccupazione è il rischio di un incrocio di informazioni (relative *in primis*, ma non solo, alla salute), idoneo a produrre effetti nella sfera giuridica dell'interessato o ad incidere in modo significativo sulla sua persona (16). Ci si intende in particolare riferire alla c.d. profilazione, notoriamente

(15) La *ratio* del divieto è rappresentata dall'oggetto del trattamento, costituito da quei dati che la Direttiva 95/46/CE definiva "sensibili". Al riguardo, degna di nota è Cass. civ., sez. un., n. 30984 del 2017, in *G. it.* 2018, 12, p. 2639, che ha chiarito il concetto di "dato sensibile" come quel dato, in particolare, in grado di rilevare lo stato di salute. Viene offerta una lettura ampia e comprensiva di qualunque informazione ritenuta particolarmente rilevante, quale la salute o l'orientamento sessuale. I dati sensibili, o categorie particolari di dati, rappresentano un *numerus clausus*: in tal senso, R. Tuccillo, *Art. 9 GDPR*, in A. Barba –S. Pagliantini (a cura di), *Delle persone*, vol. II, in E. Gabrielli (diretto da), *Commentario codice civile*, Vicenza 2019, p. 156 s. Com'è noto, a tale generale divieto fa seguito l'elencazione di una serie di deroghe ed eccezioni, che consentono il trattamento dei dati stessi. La prima ipotesi di liceità del trattamento dei dati particolari è il consenso dell'interessato; ulteriori deroghe si hanno nei casi in cui al consenso dell'interessato si sostituiscono, quali basi giuridiche del trattamento, esigenze diverse ritenute prevalenti rispetto alla posizione dell'interessato. Si tratta, specificamente, oltre alle ipotesi per l'appunto connesse con la salute, l'assistenza sanitaria e la ricerca scientifica, di quelle in cui il trattamento sia necessario per finalità relative al diritto del lavoro, alla sicurezza e alla protezione sociale; i motivi di interesse pubblico; l'esercizio o la difesa di un diritto in sede giudiziaria. Dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, sono quelli che rivelano informazioni relative al suo stato di salute (art. 4, punto 15, *GDPR*). Questi comprendono informazioni sulla persona fisica raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria o della relativa prestazione di cui alla Direttiva n. 2011/24/UE del Parlamento europeo e del Consiglio; un numero, un simbolo o un elemento specifico attribuito a una persona fisica per identificarla in modo univoco a fini sanitari; le informazioni risultanti da esami e controlli effettuati su una parte del corpo o una sostanza organica, compresi i dati genetici e i campioni biologici; e qualsiasi informazione riguardante, ad esempio, una malattia, una disabilità, il rischio di malattie, l'anamnesi medica, i trattamenti clinici o lo stato fisiologico o biomedico dell'interessato, indipendentemente dalla fonte, quale, ad esempio, un medico o altro operatore sanitario, un ospedale, un dispositivo medico o un *test* diagnostico in vitro (Considerando n. 35 *GDPR*).

(16) Ed invero, il dato personale è un concetto dinamico, che va sempre riferito al contesto, nel senso che anche un'informazione isolata può essere utilizzata tramite incrocio con altri dati. Ad esempio, le aziende di pubblicità utilizzano varie tecniche di tracciamento per poter identificare singolarmente un individuo tra i tanti navigatori *on line*: dette tecniche non permettono l'individuazione fisica della persona, ma più che altro identificano il *browser* o il dispositivo digitale tramite il quale la persona naviga in rete. Anche questi dati (*cookie*, *fingerprint*, *adid*) sono considerati dati personali. La Corte di Giustizia europea ha espressamente definito l'indirizzo IP (*Internet Protocol*) come dato personale, nella sentenza *Brever v. Germania* 2016 e il Regolamento europeo in materia di tutela dei dati personali (*GDPR*) include espressamente nei dati personali gli identificatori *on line*, quali numeri IP, *cookie* e dati di geolocalizzazione. I dati di localizzazione, o dati sulla posizione (anche dati di mobilità) sono le informazioni trattate da una rete di comunicazione elettronica o da un servizio di comunicazione elettronica che indicano la posizione geografica dell'apparecchiatura terminale (es. *smartphone*) di un utente del servizio di comunicazione elettronica. In particolare, sono i dati relativi alla: latitudine; longitudine; altitudine; direzione di marcia; ora di registrazione della posizione. Nella maggioranza dei casi tali dati derivano dai dispositivi che un utente indossa (*smart band*, *fitness tracker*, ecc.) o porta con sé (*smartphone*, *tablet*). Se raccolti in sequenza consentono di tracciare gli spostamenti delle persone nello spazio. Possono includere i dati basati su GPS da *smartphone*, *tablet* e navigatori satellitari, ma anche dalle apparecchiature *wi-fi*, ad esempio installate in locali offrendo al pubblico il servizio di connettività. I dati sulla posizione possono essere raccolti in vari modi: anzitutto, tramite *GPS* (*Global Positioning System*, cioè la rete satellitare). I dispositivi sono in grado di rilevare la propria posizione tramite la rete satellitare indipendentemente da ricezioni telefoniche o via *Internet*, l'accuratezza varia a seconda della situazione ed è influen-

definita all'art. 4, par. 4 del *GDPR* come una forma di trattamento automatizzato dei dati personali «consistente nell'utilizzo di tali dati per valutare determinati aspetti personali relativi alla persona fisica, in particolare per analizzare o prevedere aspetti riguardanti la salute [...] l'ubicazione o gli spostamenti di detta persona fisica»: processo decisionale automatizzato (profilazione) che, sotto il profilo giuridico, ai sensi dell'art. 22, par. 4, *GDPR*, coinvolgendo particolari dati personali, nella specie sanitari, sarebbe consentito, per quel che rileva ai nostri fini, ancora una volta per motivi di interesse pubblico rilevante, quale un'emergenza sanitaria, sulla base del diritto dell'Unione o degli Stati membri.

Nella specie, il rischio sarebbe rappresentato dal fatto che, attraverso algoritmi applicati all'insieme di dati sanitari di partenza riconducibili all'interessato, potrebbero ottenersi veri e propri "profili", atti a permettere valutazioni, analisi o addirittura previsioni di comportamenti (17): il che appare ancor più rischioso se si considera che le informazioni catturate dall'*app* in questione sono particolarmente dettagliate rispetto a quelle che quotidianamente giungono alle grandi corporazioni. Attraverso l'*app* "Immuni" risulta infatti possibile raccogliere e spedire al *server* informazioni accurate sulle persone con le quali si è venuti in contatto: tuttavia, ciò sarebbe fondato se e nella misura in cui fosse stato adottato un sistema centralizzato di tracciamento, laddove il nostro Governo ha optato per un protocollo (anche se non del tutto, comunque) decentralizzato, nel quale i dati non dovrebbero (il condizionale è d'obbligo) transitare fuori dal *device* dell'utente, con conseguente maggiore sicurezza e affidabilità per gli interessati e utenti dell'*app*; inoltre, stando a quanto riportato dal Ministero della Salute, il *software* di *contact tracing* sarebbe stato sviluppato soltanto per registrare la prossimità tra cellulari delle persone con i quali un soggetto è venuto in contatto, tramite dati non direttamente idonei a rivelare l'identità di una persona: dati che per l'appunto dovrebbero rimanere solo nel cellulare fino all'eventuale diagnosi di contagio (18). L'*app* "Immuni" non dovrebbe raccogliere alcun dato che consenta di risalire all'identità di un utente (19) e tutti i dati, siano essi salvati sul dispositivo o sul *server*, dovrebbero essere cancellati non appena non più necessari. È il Ministero della Salute il soggetto che raccoglie i dati dell'utente, che verranno usati solo per contenere l'epidemia del *Co-*

zata da condizioni meteorologiche o interferenze (nelle città è meno preciso), per cui gli *smartphone* utilizzano il GPS in abbinamento con altre tecnologie per rendere più preciso il dato; tramite le torri cellulari utilizzate per la fornitura del servizio di comunicazione cellulare, sicché i gestori di telefonia sanno sempre approssimativamente dove si trova un dispositivo perché questo dialoga continuamente con le torri (che emettono costantemente degli "ID *Tower*" unici, *Open Cell ID* per conoscere le torri vicine alla tua posizione), e ciò è necessario per poter instradare la comunicazione (telefonica o *Internet*). Dalla presenza in una "cella" e dalla forza del segnale può essere dedotta approssimativamente la posizione del dispositivo. Di questo tracciamento l'operatore tiene un registro che può essere consultato solo dalle forze di polizia: tramite reti *wi-fi*, i dispositivi mobili possono ricavare la loro posizione eseguendo la scansione delle reti *wi-fi* (o dei punti di accesso) nelle vicinanze, esistono molti *database* dei *router wireless*; tramite *Beacon Bluetooth*, là dove i "*beacon*" sono piccoli trasmettitori radio che usano segnali *Bluetooth* unidirezionali, che possono essere collegati a vari oggetti (chiavi, portafoglio), installati in luoghi (es. negozi) e, se l'utente acconsente alla connessione *Bluetooth*, possono trasmettere informazioni, consentendo di dedurre la posizione del dispositivo; tramite una combinazione di segnali: i moderni *smartphone* combinano più segnali dalle fonti sopra indicate per calcolare la posizione in maniera più precisa, anche accorpando le informazioni fornite dagli innumerevoli sensori (altimetro, accelerometro).

(17) L'interesse primario delle aziende è essenzialmente sapere chi è l'utente, "profilarlo", per poi mostrargli pubblicità corrispondenti ai relativi interessi; lo Stato potrebbe abusare delle informazioni e dei dati personali, con conseguente grave pericolo per la tutela della *privacy*, in nome di una discutibile e magari infondata ragione di pubblica sicurezza.

(18) Volendo esemplificare, X e Y sono due ipotetici utenti: una volta installata da X, l'*app* fa in modo che il suo *smartphone* emetta continuativamente un segnale *Bluetooth Low Energy* che include un codice casuale. Lo stesso vale per Y. Quando X si avvicina ad Y, gli *smartphone* dei due utenti registrano nella propria memoria il codice casuale dell'altro, tenendo quindi traccia di quel contatto. Registrano anche quanto è durato il contatto e a che distanza erano i due *smartphone* approssimativamente. I codici dovrebbero essere generati a caso, senza contenere alcuna informazione sul dispositivo o l'utente. Inoltre, essi dovrebbero essere modificati diverse volte ogni ora, in modo da proteggere ulteriormente la *privacy* degli utenti. Supponiamo che, successivamente, Y risulti positivo al *Covid-19*. Con l'aiuto di un operatore sanitario, Y potrà caricare su un *server* delle chiavi crittografiche dalle quali è possibile derivare i suoi codici casuali. Per ogni utente, l'*app* scarica periodicamente dal *server* le nuove chiavi crittografiche inviate dagli utenti che sono risultati positivi al *virus*. L'*app* usa queste chiavi per derivare i loro codici casuali e controllare se qualcuno di quei codici corrisponde a quelli registrati nella memoria dello *smartphone* nei giorni precedenti. In questo caso, l'*app* di X troverà il codice casuale di Y, verificherà se la durata e la distanza del contatto siano state tali da aver potuto causare un contagio e, se sì, avvertirà X.

(19) A quanto pare, il sistema non chiede nome, cognome, data di nascita, indirizzo, numero di telefono o indirizzo *email*. L'*app* chiede solo la Regione e la Provincia in cui ci si trova. L'*app* non raccoglie nemmeno alcun dato di geolocalizzazione, inclusi i dati del GPS: gli spostamenti non sembrerebbero tracciati in alcun modo. Il codice *Bluetooth Low Energy* trasmesso dall'*app* risulta generato in maniera casuale, senza alcuna informazione riguardo allo *smartphone*, né alla persona. Inoltre, questo codice dovrebbe cambiare diverse volte ogni ora, per tutelare meglio proprio la *privacy*. I dati salvati sullo *smartphone* risultano cifrati, così come le connessioni tra l'*app* e il *server*.

vid-19 o per la ricerca scientifica e che saranno salvati su *server* in Italia e gestiti da soggetti pubblici.

4. (*Segue*). Le garanzie per l'interessato: limitazione della finalità, minimizzazione e anonimizzazione dei dati personali

Vagliata la base giuridica dell'*app* "Immuni", occorre a questo punto spostare il piano della riflessione sulle garanzie necessarie affinché il trattamento, oltreché lecito, sia conforme al *GDPR* e in grado di assicurare al tempo stesso quel necessario bilanciamento tra tutela della salute pubblica e protezione della sfera privata da un'eccessiva compressione o invadenza. Più precisamente, l'*app* "Immuni", così come eventuali altri sistemi di tracciamento ritenuti leciti, dovrebbe essere utilizzata nel rispetto non solo del principio di liceità, ma anche di quello di limitazione della finalità, di minimizzazione e di anonimizzazione.

Procedendo con ordine, in forza del principio di limitazione della finalità, attraverso l'*app* "Immuni", i dati personali devono essere trattati e raccolti per uno scopo esplicito, consistente nel monitorare¨, contenere e mitigare il contagio da *Covid-19*: ciò, al fine di tutelare la salute pubblica, e non certo controllare o stigmatizzare le persone, reprimendone o spiandone di fatto i comportamenti. La finalità del trattamento, determinata *ex ante*, costituisce così una garanzia specifica per i soggetti interessati dal trattamento.

Più precisamente, ai sensi dell'art. 5, par. 1, lett. *b*), i dati sanitari devono essere raccolti per quella particolare «finalità determinata, esplicita e legittima», e successivamente trattati in modo non incompatibile con tale finalità: il nucleo essenziale della *compliance* dell'*app* "Immuni" con il Regolamento risulta quindi rappresentato dalla determinatezza del fine esplicito sotteso alla raccolta e dalla compatibilità del trattamento con questo fine. Un problema di compatibilità potrebbe invece porsi per «un ulteriore trattamento» o riutilizzo dei dati "sensibili" per un fine diverso da quello espresso, come ad esempio di ricerca scientifica: riutilizzo «considerato *di per sé* non incompatibile con le finalità iniziali» dall'art. 5, par. 1, lett. *b)* e dall'art. 110-*bis* [introdotto dall'art. 28, comma 1, lett. *b*), legge n. 167 del 2017] del Codice in materia di protezione dei dati personali (d. legisl. n. 196 del 2003), che per l'appunto lo legittimano per fini di ricerca scientifica, sia pur con l'autorizzazione del Garante e con l'adozione di tecniche di minimizzazione e di anonimizzazione ritenute idonee per tutelare gli interessati (20).

In particolare, il principio di minimizzazione impone di contenere o limitare i dati trattati mediante l'*app* "Immuni" a quelli necessari e indispensabili per il raggiungimento dello scopo dichiarato, vale a dire il contenimento dell'epidemia da *coronavirus*. Ciò incide sul periodo di tracciamento oltreché di conservazione dei dati, che deve essere temporalmente circoscritto al minimo necessario, ossia al lasso strettamente indispensabile e individuato (nella specie), dall'Autorità Garante, nella fine dell'emergenza: da qui, il rischio di un'eccessiva dilatazione temporale in funzione di un'eventuale prosecuzione *sine die* dell'emergenza, stante la fissazione seppur *ex ante* di un *dies ad quem* periodicamente spostato in avanti. Come raccomandato dall'Autorità Garante, l'attuale crisi sanitaria non può e non deve trasformarsi in un'occasione per derogare al principio di minimizzazione e conseguente limitazione del trattamento e della conservazione dei dati: entrambi (trattamento e conservazione) dovrebbero cioè essere limitati alla luce delle reali esigenze e della rilevanza medica, ossia esclusivamente per la durata della crisi dovuta al *Covid-19*, anche con riguardo a considerazioni di natura epidemiologica quali il periodo di incubazione. Successivamente, tutti i dati personali dovrebbero essere cancellati (21). Ai sensi dell'art. 5, par. 1, lett. *c*), il principio di minimizzazione si declina dunque nel canone della "necessità": sicché se, per l'appun-

(20) Testualmente, «il Garante può autorizzare il trattamento ulteriore di dati personali, compresi quelli dei trattamenti speciali di cui all'art. 9 del Regolamento, a fini di ricerca scientifica o a fini statistici da parte di soggetti terzi che svolgano principalmente tali attività quando, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca, a condizione che siano adottate misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, in conformità all'art. 89 del Regolamento, comprese forme preventive di minimizzazione e di anonimizzazione dei dati».

(21) Così ad esempio, qualora si richieda il rilascio di una dichiarazione attestante la non provenienza dalle zone a rischio epidemiologico e l'assenza di contatti, negli ultimi 14 giorni, con soggetti risultati positivi al *Covid-19*, si ricorda di prestare attenzione alla disciplina sul trattamento dei dati personali, poiché l'acquisizione della dichiarazione costituisce un trattamento dati. A tal fine, si suggerisce di raccogliere solo i dati necessari, adeguati e pertinenti rispetto alla prevenzione del contagio da *Covid-19*. Se si richiede una dichiarazione sui contatti con persone risultate positive al *Covid-19*, occorre astenersi dal richiedere informazioni aggiuntive in merito alla persona risultata positiva; oppure, se si richiede una dichiarazione sulla provenienza da zone a rischio epidemiologico, è necessario astenersi dal richiedere informazioni aggiuntive in merito alle specificità dei luoghi (Prot. 24 aprile 2020, nota 2). In

to, la finalità è quella di contenere i contagi, gli unici dati personali che dovrebbero essere acquisiti sono quelli sanitari e tali informazioni possono essere utilizzate esclusivamente per ridurre il rischio epidemiologico. Ogni eventuale ulteriore dato oppure ogni ulteriore utilizzo dei dati personali determinerebbe una violazione del principio in esame, e quindi del *GDPR*, perché eccedente rispetto a quanto strettamente "necessario" per il raggiungimento di quella finalità come predeterminata e comunicata all'interessato (vale a dire, la lotta al *Covid-19*). Questo non significa che eventualmente non possano essere raccolti altri dati o trattare quelli raccolti in modo diverso, ma in tali casi, per ciascuno di essi, occorrerà ottenere il consenso dell'interessato o basarsi su un'altra delle condizioni di liceità previste dal Regolamento, diversa da quella legittimante il trattamento dei dati sanitari e individuata nell'art. 9.2, lett. *i)*, del *GDPR*.

In merito all'utilizzo dei dati, e in particolare all'*app* "Immuni", lo *EDPB* e l'associazione *European Digital Right* raccomandano poi la forma anonima, là dove per "anonimizzazione" si intende l'uso di una serie di tecniche finalizzate ad eliminare la possibilità di collegare i dati a una persona fisica identificata o identificabile con uno sforzo "ragionevole" (22): ragionevolezza valutata alla luce di aspetti oggettivi (quali tempi e mezzi tecnici, rarità di un fenomeno, densità di popolazione, natura e volume dei dati). In caso di esito positivo di siffatta valutazione, i dati non saranno anonimizzati (23).

Se è vero che i dati relativi all'ubicazione provenienti da operatori delle telecomunicazioni e/o da servizi della società dell'informazione sono notoriamente difficili da anonimizzare in quanto la sequenza dei dati consente di ricostruire i movimenti di una determinata persona nel tempo (es. casa-lavoro), è altrettanto vero che l'*app* "Immuni" non *dovrebbe* raccogliere alcun dato idoneo a consentire di risalire all'identità di un utente. Tale sistema di trattamento, ad esempio, non chiede né risulta congegnato in modo da ottenere nome, cognome, data di nascita, indirizzo, numero di telefono o indirizzo *email*, dati di geolocalizzazione o GPS: gli spostamenti non sembrano tracciati né tracciabili. L'*app* "Immuni" richiede solo la Regione o la Provincia in cui ci si trova e il codice *Bluetooth Low Energy* trasmesso dall'*app* appare generato in maniera casuale, privo di qualunque informazione riguardo allo *smartphone* o alla persona. Inoltre, questo codice cambia diverse volte, a intervalli temporali brevi, proprio per tutelare la *privacy*. I dati salvati sullo *smartphone* sono cifrati, così come le connessioni tra l'*app* e il *server* (24): tutto ciò dovrebbe garantire l'anonimizzazione dei dati.

I termini del discorso e l'effettività della tutela dei dati personali cambierebbero in negativo se i dati

merito al trattamento di dati personali relativi alla localizzazione tramite telefonia mobile, l'*EDPB* avverte che le misure legislative introdotte per salvaguardare la sicurezza pubblica devono avere carattere eccezionale e devono essere "necessarie", proporzionate e adeguate. Lo *EDPB* e il Garante per la protezione dei dati personali hanno altresì raccomandato il rispetto del principio di *trasparenza* e di *esattezza* dei dati trattati nell'adozione delle misure tecnologiche emergenziali nei confronti degli interessati. Com'è noto, il primo, privo di un'espressa enunciazione nella disciplina previgente, è ora esplicitamente menzionato in termini sia generali, all'art. 5, là dove viene imposto al titolare l'obbligo di trattare i dati in modo "trasparente"; sia più specifici, all'art. 12, alla cui stregua le informazioni e comunicazioni cui ha diritto l'interessato devono essere fornite «in forma [...] trasparente». In particolare, l'art. 12 individua modalità e caratteristiche necessarie affinché sia garantita un'informazione per l'appunto "trasparente": le informazioni devono essere concise e facilmente accessibili, il linguaggio utilizzato deve essere chiaro e comprensibile anche per i non addetti ai lavori (specie se si tratta di minori), strutturato in modo semplice, evitando frasi complesse, termini astratti o ambigui che lascino spazio a molteplici interpretazioni. Il principio dell'*esattezza* impone che i dati siano corretti, quindi aggiornati, rettificati e anche cancellati se inesatti rispetto alla finalità per la quale vengono trattati: sul punto, cfr. D. Achille, *Art. 12*, in E. Gabrielli (diretto da), *Commentario del codice civile*, cit., p. 208.

(22) La ragionevolezza è un criterio relativo e "ragionevole" significa che la probabilità che l'evento si verifichi è più elevato rispetto alla mera probabilità. Nel concetto è ricompreso qualsiasi processo anche meramente deduttivo attraverso il quale è possibile approdare all'identificazione. Quando tale approdo o collegamento si interrompe, si parla di anonimizzazione. Il Considerando n. 26 esclude l'applicazione della disciplina della protezione dei dati a informazioni anonime, vale a dire informazioni che non si riferiscono ad una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato: sull'argomento, v. G.M. Riccio – G. Scorza – E. Belisario (a cura di), *GDPR e normativa* Privacy *commentario*, Vicenza 2018, p. 29 ss.

(23) E. Pelino, *Informazioni anonime, dati anonimizzati*, in L. Bolognini –C. Bistolfi – E.Pelino, *Il Regolamento* Privacy *europeo*, Milano 2016, p. 74: l'anonimizzazione è un trattamento cui sono sottoposti i dati personali, volto ad ottenerne la deidentificazione irreversibile del soggetto cui l'informazione si riferisce. Dato "anonimo" è «il dato che in origine, o a seguito di trattamento, non può essere associato a un interessato identificato o identificabile»: sull'argomento, cfr. per tutti, Finocchiaro (a cura di), *Diritto dell'anonimato. Anonimato, nome e identità personale*, in Galgano (diretto da), *Trattato di diritto commerciale e diritto pubblico dell'economia*, XLVIII, Padova 2008.

(24) Ciononostante, trattandosi di un sistema ancora in rodaggio, diverse sono le questioni ancora irrisolte. Anzitutto appare legittimo chiedersi se i dati, visto che risiederanno nel singolo telefono sia pur in forma anonima, potranno essere prelevati da altre *app* che tradizionalmente richiedono l'accesso per usufruire del singolo *software* e che, incrociando i dati con altri relativi al telefono (IP, scheda SIM, foto, *etc*.), potrebbero utilizzarli in maniera impropria. Sembrerebbe che, sebbene i singoli dati siano crittografati, non si possa escludere una de-anoni-

oggetto di tracciamento (anziché anonimizzati) venissero soltanto pseudonimizzati (25). Sebbene, infatti, la pseudonimizzazione sia «ideale per aumentare la protezione dei dati» (26), essa consentirebbe tuttavia di risalire alla persona per scoprirne l'identità (27), specie là dove vengano utilizzate liste di corrispondenza delle identità con i relativi pseudonimi, o algoritmi crittografici bidirezionali (28): ciò, a differenza dell'anonimizzazione, caratterizzata essenzialmente da una "de-identificazione" irreversibile, come sembra doversi qualificare quella scaturente dall'*app* "Immuni".

Sul piano dell'efficacia, anche alla luce delle riflessioni sin qui svolte, l'*app* "Immuni" presenta diversi nodi ancora da sciogliere. Al riguardo, il Ministro per l'Innovazione Tecnologica ha precisato che la soglia (condivisa anche dal Garante *Privacy*) di efficacia dell'applicativo è l'adozione da parte di almeno il 60-70% degli italiani (29): l'*app* "Immuni" funziona, cioè, solo se si raggiunge una massa critica di utenti dell'applicazione (30). Trattandosi di uno strumento del tutto volontario e visto che non tutte le fasce di popolazione hanno adeguata dimestichezza con gli *smartphone*, è evidente che il problema principale (dalla cui soluzione dipende il successo o il fallimento dell'applicazione) è proprio quello di raggiungere questa soglia di adesione, anche mediante misure che incentivino il *download* dell'applicazione purché lecite e conformi ai principi vigenti in materia (31).

Altro problema da non sottovalutare è quello degli strumenti complementari a supporto dell'iniziativa di *contact tracing*. L'efficienza della soluzione tecnologica, e in particolare dell'*app* "Immuni", non può prescindere né dall'effettuazione di controlli, tramite tamponi, per individuare i positivi e per isolare i casi meno gravi, per i quali l'assistenza sanitaria dovrebbe avvenire a domicilio e assicurando un rapido tampone a chi ha ricevuto la notifica (*testing*); né da un sistema di tracciamento più ampio, fatto anche di controlli manuali e di gestione dei *big data* epidemiologici (*tracing*). L'*app* "Immuni" si rivela poi inefficace se non accompagnata e supportata da azioni positive (es. contattare e sottoporre a tampone tutti i soggetti che hanno avuto contatti con un contagiato nelle due settimane precedenti) (32).

mizzazione e riconduzione alle identità dei singoli e ai dati sanitari sui contagi, eseguendo una manipolazione di milioni di questi dati incrociati.

Altro rischio sembra rappresentato da una possibile intrusione mediante il *bluetooth* di c.d. *sniffer* (intercettatori) in grado di intercettare i dati. È noto che il *bluetooth* sia un canale di comunicazione utilizzato non solo per interconnettere altri dispositivi come gli auricolari, ma anche per il passaggio di dati tra persone vicine: da qui, il problema della sicurezza di questo canale di comunicazione utilizzato per l'*app* "Immuni". Infine, un'ulteriore questione attiene al *server* che verrà utilizzato per immagazzinare i dati: *server* che, opportunamente, dovrebbe risiedere in Italia e gestito dalla P.A., in particolare dal Ministero della Salute, e non da aziende specie se straniere che potrebbero averne accesso e prelevare i dati per altri scopi.

(25) L'art. 4, n. 5, *GDPR* definisce la pseudonimizzazione come quel trattamento dei dati personali in modo tale che i dati personali non possano essere più attribuiti ad un interessato specifico senza l'utilizzo di informazioni aggiuntive.

(26) Così, G.M. Riccio – G. Scorza – E. Belisario (a cura di), *GDPR e normativa* Privacy *commentario*, cit., p. 41.

(27) «Per converso, è possibile mascherare l'identità rendendo impossibile la ri-identificazione, per esempio con la crittografia unidirezionale che crea in genere dati anonimi»: così, C. Del Federico – A.R. Popoli, *Disposizioni generali*, in G. Finocchiaro, *Il nuovo Regolamento europeo sulla* Privacy *e sulla protezione dei dati personali*, Bologna 2017, p. 97.

(28) Con la pseudonimizzazione si ha il mantenimento di un dato, che viene sostituito con uno pseudonimo e realizzato con diverse tecniche, come ad esempio la crittografia, *hashing*, ecc. In questo caso, al contrario del dato "anonimizzato", è possibile in maniera indiretta risalire al contenuto originale, se si hanno le chiavi di decifratura dell'algoritmo utilizzato. Un dato pseudonimizzato si basa prevalentemente su tre caratteristiche: l'individuazione, ossia la possibilità di identificare i dati iniziali delle persone, la correlabilità con il dato originale e la deduzione, qualora ad esempio l'attributo sostituito presenti delle analogie con l'originale, oppure integrando diversi dati si deduce quale è la fonte.

(29) Secondo certi esperti del sistema sanitario nazionale inglese, comunque, il 40% darebbe vantaggi nel ridurre le vittime, addirittura del 30%.

(30) Solo un'*app* efficace sul punto, insieme ad una comunicazione altrettanto efficace delle soluzioni adottate, potrà accompagnare gli utenti verso un'adozione graduale ma massiccia di questo importante strumento per la lotta alla diffusione del *Covid-19*.

(31) Allo stato attuale, l'*app* di *contact tracing* (disponibile dal 15 giugno 2020 su tutto il territorio) supera di poco i 4 milioni di *download*. Il sistema di monitoraggio del contagio non ha quindi finora fatto breccia e, a fronte di nuovi focolai di *Covid* scoppiati nel Paese, soddisfa ben poco, anche per il cattivo funzionamento secondo quanto riportato dai giornali: da qui, la necessità, da un lato, di un'*app* unica anziché di sistemi di tracciamento simili a livello regionale (come in Lombardia, Sicilia e Sardegna), con esiti differenziati tra i cittadini a seconda della diffusione del contagio; dall'altro, del miglioramento del sistema e della possibilità di installarla su tutti i dispositivi, incrementando la fiducia dei cittadini in questo sistema di monitoraggio, ancora troppo diffidenti e timorosi di possibili violazioni della *privacy*, a poco valendo finora le rassicurazioni diffuse al riguardo mediante i diversi mezzi di informazione.

(32) Tali azioni, peraltro, non possono essere particolarmente penalizzanti, altrimenti si otterrebbe, presumibilmente, un drastico calo delle adozioni. Questo "rilevatore" sempre a portata di mano potrebbe indurre a modificare i propri comportamenti, magari spostandoci a una distanza superiore a quella di sicurezza dalle altre persone per evitare che anche brevi contatti ininfluenti (pensiamo ad un passante incrociato su un marciapiede o all'affiancamento di una vettura in un parcheggio) possano "marcarci" come positivi, se da un lato questo può aiutare nell'efficacia delle marcature, si tratta di un aspetto che potrebbe generare tensioni. Né appare risolutivo, al riguardo, richiamare il principio di responsabilizzazione o "*ac-*

In conclusione, censurato, come parrebbe, l'utilizzo di soluzioni che consentano l'accesso alla posizione dell'individuo, l'augurio è che lo scopo dell'*app* "Immuni"– e di altre eventuali future e/o diverse applicazioni – rimanga quello di scoprire "eventi", e cioè i contatti con contagiati, e non movimenti, spostamenti o comportamenti dei soggetti interessati, evitando altresì la diffusione di allarme sociale e la stigmatizzazione dei soggetti risultati positivi: l'unica finalità in nome della quale legittimare in astratto e in concreto una compressione della libertà personale deve essere e rimanere espressamente soltanto quella di poter risalire la catena dei potenziali contagiati e adottare le misure appropriate al contenimento della pandemia.

countability": non è un problema di definizione chiara né di individuazione della titolarità del trattamento di un'*app* per il tracciamento di contatti, quanto il fatto che un'*app* per il tracciamento dei contatti comporta la memorizzazione e/o l'accesso a informazioni particolari. Il Comitato ritiene peraltro che le autorità sanitarie nazionali debbano essere i titolari di tale trattamento; si potranno comunque prendere in considerazione altre configurazioni di titolarità.