IL TRATTAMENTO DEI DATI INERENTI ALLA SALUTE NELL'EPOCA DELLA PANDEMIA: CRONACA DELL'EMERGENZA

Di Dianora Poletti

ABSTRACT. L'esigenza di fronteggiare lo stato di pandemia con disposizioni di rango legislativo (e non solo) ha incisivamente investito la disciplina della protezione dei dati personali e in particolare dei dati di tipo sanitario. Anche se le autorità europee hanno tracciato le coordinate di un approccio "pan-europeo" che, anche al tempo del Covid-19, mira a non sacrificare i principi fondamentali del trattamento (in particolare quello di proporzionalità), il diritto alla protezione dei dati personali sta affrontando una prova importante, nella quale il confronto con la tutela della salute collettiva rischia di trasformare il possibile bilanciamento in compressione delle sue essenziali garanzie.

The need to face the pandemic situation trough legislative provisions (and not only), has incisively affected the discipline of data protection, in particular of health data. Although the European authorities built the foundations of a "pan-European" approach which, even at the time of Covid-19, aims not to sacrifice the fundamental principles of processing, especially the proportionality, data protection is facing a crucial test, where the comparison with the protection of collective health threatens to transform the possible balance into a compression of data protection core guarantees.

1. Legislazione di emergenza e dati personali.

Una delle principali risposte delle autorità pubbliche alla drammatica situazione determinata dal Covid-19 è l'uso di soluzioni che combinano soluzioni tecnologiche, anche con il ricorso all'intelligenza artificiale, e utilizzo dei dati. La frenesia legislativa imposta dal momento attuale, volta ad arginare il dilagare del virus, ha anzitutto investito, in maniera incisiva, la protezione dei dati personali e in particolare dei dati inerenti alla salute.

La raccolta ad oggi delle principali disposizioni adottate in relazione allo stato di emergenza epidemiologica aventi implicazioni in materia di protezione dei dati personali operata dall'Autorità garante, a partire dalla dichiarazione di emergenza in conseguenza del rischio sanitario assunta con delibera del Consiglio dei Ministri del 31 gennaio 2020, conta oltre duecentocinquanta pagine[1]. Questa regolazione frammentata, a volte abrogata e poi riproposta, dispersa tra le pieghe di decreti del Presidente del Consiglio dei Ministri, decreti legge, decreti ministeriali, ordinanze del Capo Dipartimento della Protezione Civile, circolari ministeriali, direttive del Dipartimento della Funzione pubblica, protocolli vari, in via di progressiva e rapida implementazione, richiede già di per sé uno sforzo di sistemazione non indifferente.

Il nucleo fondamentale delle soluzioni normative raggiunte in tema di protezione dei dati personali a livello europeo, tutte giocate su un delicato equilibrio tra necessità o intento di trattare i dati personali altrui e riservatezza delle informazioni, è evidentemente messa a dura prova nel momento attuale, nel quale la protezione dei dati personali rischia di venire ridotta a elemento di intralcio alle iniziative di contenimento della crisi sanitaria. Il problema è quindi l'individuazione del punto di compressione del diritto di fronte a prioritarie esigenze di tutela della sicurezza e della salute collettiva.

La tutela dei dati personali, mai come oggi, non deve essere considerata un feticcio da preservare in ogni caso né, all'opposto, un abito delle feste che, in tempi di pandemia, non è più consentito indossare.

Lo scenario è ancora più complesso, perché coinvolge non solo il settore del trattamento dei dati personali, con la relativa disciplina, ma più in generale l'impiego dei dati anche non personali e dei *big data*, con la loro capacità predittiva, ai fini di contrasto alla pandemia. La brusca accelerazione dello *smart working*, l'impiego diffuso dell'*e-learning*, cui si può aggiungere l'impennata dell'*e-commerce* a causa della limitata circolazione delle persone, ha generato una fortissima spinta alla digitalizzazione e l'immissione in rete di quantitativi impressionanti di dati personali, di conoscenza e di sapere, sortendo un effetto la cui portata non è forse stata appieno compresa nel suo significato più profondo e preoccupante. Piattaforme private come Google Meet, Zoom, con i problemi che già si sono generati, Microsoft teams, Skype for business, vengono messe a disposizione (gratuitamente?) delle autorità pubbliche per la gestione di servizi come la scuola, l'università, la sanità, le attività della pubblica amministrazione, lo svolgimento delle udienze penali e civili[2], sollevando l'interrogativo se tali piattaforme rappresentino forniture di servizi essenziali di pubblica utilità, tanto da ipotizzare la loro trasformazione in *utilities*[3]. La mancanza di piattaforme e infrastrutture informatiche pubbliche ha denunciato in modo evidente il *deficit* tecnologico del nostro Paese.

2. Dati sanitari, ricerca scientifica e Covid-19.

In tempi di pandemia il problema più scottante è rappresentato dal trattamento dei dati inerenti alla salute, categoria "particolare" di dati nella quale sono più stringenti le condizioni che legittimano il

[1] Garante privacy, Raccolta delle principali disposizioni adottate in relazione allo stato di emergenza epidemiologica da Covid-19 aventi implicazioni in materia di protezione dei dati personali, aggiornata al 29 aprile 2020.

[2] Cfr. il provvedimento del 20 marzo 2020 del Direttore generale per i sistemi informativi automatizzati del Ministero della Giustizia, che individua in Skype for business e Teams di Microsoft le piattaforme da utilizzare per lo svolgimento delle udienze civili, in applicazione di quanto disposto dall'art. 83 c. 7 del d.l. 17 marzo 2020, n. 18 (convertito dalla legge 24 aprile 2020, n. 27 e in parte modificato, ma non per i profili qui in esame, dal d.l. 30 aprile 2020, n. 28). Il provvedimento precisa che "i collegamenti effettuati con i due programmi su dispositivi dell'ufficio o personali utilizzano infrastrutture di questa amministrazione o aree di data center utilizzate in via esclusiva al Ministero della giustizia". Il 16 aprile 2020 il Garante Privacy, del quale non è stato chiesto il parere, ha inviato al Ministero della Giustizia una nota nella quale sono stati manifestati dubbi sull'"opportunità della scelta di un fornitore del servizio in questione (Microsoft Corporation, *ndr*) stabilito negli Usa e, come tale, soggetto tra l'altro all'applicazione delle norme del Cloud Act (che come noto attribuisce alle autorità statunitensi di contrasto un ampio potere acquisitivo di dati e informazioni)".

[3] O. POLLICINO, *Una nuova applicazione mobile per Giustizia insieme fa riflettere su distonie e utopie del rapporto tra tecnologia e società*, in *Giustizia insieme*, 18 aprile 2020, evidenzia come queste piattaforme stiano fornendo servizi essenziali di pubblica utilità, senza alcun contratto, onere o particolare responsabilizzazione in questo senso, aggiungendo "se diventano *digital utilities* adesso, come a tutti gli effetti stanno diventando, nel post-emergenza dovranno essere di conseguenza pesantemente regolate, come lo è chi fornisce servizi pubblici essenziali".

trattamento e più incisive le tutele dell'interessato, che nel momento attuale sono necessari a una molteplicità di soggetti per il compimento di attività di contenimento e di mitigazione dei rischi per le persone.

In questa sede l'attenzione verrà dedicata esclusivamente a questo tipo di dati, e sarà necessariamente una attenzione solo parziale, perché alcuni profili saranno volutamente esclusi[4], tanto che la cronaca di cui si fa menzione nel titolo del contributo sarà inevitabilmente incompleta[5].

La protezione di questi dati ha subito, nell'immediatezza delle reazioni alla diffusione del contagio, un processo di compressione normativa, al quale ha fatto seguito un frastagliamento applicativo.

Per un primo decreto legge, seguito dalla legge di conversione di un decreto successivo (il c.d. "Cura Italia")[6], la Protezione civile, il Ministero della Salute, l'Istituto superiore di sanità, le strutture pubbliche e private che operano nell'ambito del Servizio sanitario nazionale, i soggetti attuatori individuati dal Capo del Dipartimento della Protezione civile anche tra enti pubblici economici e non economici e soggetti privati, che agiscono sulla base di specifiche direttive, nonché i soggetti deputati a monitorare e a garantire l'esecuzione delle misure disposte ai sensi dell'articolo 2 del decreto-legge 25 marzo 2020, n. 19 (ossia i prefetti, che si possono avvalere delle forze di polizia e di altri soggetti), possono infatti procedere alla comunicazione tra loro di tutte le categorie particolari di dati personali di cui all'art. 9 del Regolamento, tra cui dati inerenti alla salute e dati biometrici, oltre che ai dati relativi alle condanne penali e ai reati di cui all'art. 10 del regolamento stesso, per finalità di prevenzione dell'epidemia.

La necessità di assicurare la gestione dei flussi e l'interscambio di dati personali legittima, in fase di emergenza sanitaria, anche la comunicazione e persino la diffusione dei dati diversi da quelli sopra menzionali a soggetti pubblici e privati, sempre per finalità indispensabili allo svolgimento delle attività connesse alla gestione di tale emergenza.

Le autorizzazioni generali di cui all'art. 2-*quaterdecies* del d. lgs. n. 196/2003 possono essere rilasciate anche oralmente e l'informativa – principio cardine dell'intera normativa in materia – può essere omessa o fornita in via semplificata. La norma stabilisce inoltre che alla fine dell'emergenza il trattamento di dati personali effettuati nel periodo dovrà essere ricondotto "all'ambito delle ordinarie competenze e delle regole che disciplinano i trattamenti di dati personali", dichiarando apertamente il suo carattere straordinario.

Mentre riduce le protezioni dell'interessato, la previsione amplia sia il novero dei soggetti titolari di un potere emergenziale di intervento sia gli strumenti normativi utilizzabili, individuati in tutti i provvedimenti di urgenza che pressoché chiunque abbia compiti relativi alla lotta al Codiv-19 può adottare.

L'assenza di misure di garanzia da impiegare nella gestione dell'emergenza ha finito per assegnare alla norma un improprio carattere "liberatorio" del trattamento dei dati personali, che ha generato il proliferare di autonome iniziative, persino differenziate da zona a zona. Nel contesto da essa tratteggiato hanno infatti trovato rassicurante collocazione le varie ordinanze di Presidenti di regione, alcune già adottate in precedenza.

Mentre dall'Europa si intensificavano i richiami a regolamentazioni dell'emergenza omogenee nel contesto eurounitario quanto al trattamento dei dati personali, il nostro Paese ha iniziato a registrare quello che è stato definito un processo di "geopardizzazione" dei diritti, attuato tra l'altro tramite fonti secondarie e soprattutto atti di natura amministrativa[7], che hanno rivelato un carattere fortemente declinante delle fonti di rango primario.

Eppure, la protezione dei dati personali, anche di quelli appartenenti alle categorie particolari di dati personali, come i dati sanitari, non ha mai rivestito un carattere di assolutezza, come più volte riconosciuto anche dalla Corte di Giustizia dell'Unione Europea, posto che molti valori (tra questi, proprio la sicurezza pubblica e la salute collettiva) sono atti a operare un bilanciamento con questa tutela. Basterebbe ricordare, preceduti dal Considerando 46 che menziona espressamente la pandemia[8], l'art. 6, par.

[4] Come quello relativo al trattamento dei dati inerenti alla salute da parte dei datori di lavoro, foriero di rilevanti ripercussioni, sul quale v., per una prima considerazione, E. DAGNINO, *La tutela della* privacy *ai tempi del coronavirus: profili giuslavoristici*, in *Giustizia civile.com*, Emergenza Covid-19 -Speciale, n. 1/2020, p. 61 ss.

[5] Si avverte che anche l'apparato di note del presente contributo è limitato all'essenziale, con preferenza per gli scritti, anche di pronta pubblicazione, che hanno riguardato l'emergenza Covid-19.

[6] Si fa riferimento all'art. 14 del d.l. 9 marzo 2020, n. 14, varato dal Governo per il potenziamento del sistema sanitario nazionale di fronte all'espandersi dei contagi, che da veste normativa ad una precedente ordinanza (3 febbraio 2020) del Dipartimento della Protezione civile. Il d.l. è stato abrogato dalla l. 24 aprile 2020, n. 27, di conversione del d.l. 17 marzo 2020, n. 18 (c.d. Cura Italia). L'art. 17-*bis* della legge di conversione ripropone interamente il contenuto dell'art. 14 del d.l. n. 14/2020.

[7] F. Pizzetti, *A rischio le libertà dei cittadini: urgente un intervento giuridico*, in *Agendadigitale.eu*, 23 marzo 2020.

[8] "...Alcuni tipi di trattamento dei dati personali possono rispondere sia a rilevanti motivi di interesse pubblico sia gli interessi vitali dell'interessato, per esempio se il trattamento è necessario a fini umanitari, tra l'altro per tenere sotto controllo le

1, specie lettere c) ed e) e l'art. 9, par. 2, lettere c), g), h), i) del Regolamento generale 2016/679 (GDPR) sulle basi giuridiche che legittimano il trattamento, rispettivamente dei dati "comuni" e dei dati "particolari", l'art. 23 riguardante le limitazioni legislative degli obblighi e dei diritti oppure considerare, per il diritto italiano, l'art. 2 *sexies*, lettere u), v), z) del Codice privacy ("Trattamento di categorie particolari di dati personali necessari per motivi di interesse pubblico rilevanti").

Il GDPR contiene inoltre più di una disposizione in merito al trattamento dei dati relativi alla salute per perseguire scopi di ricerca scientifica, adatte a governare anche il contesto dell'emergenza generata dal Covid-19 (riconosciuta dall'UE e dalla maggior parte dei suoi Stati membri come un interesse pubblico rilevante) specie per creare mappe epidemiologiche e documentare il percorso del contagio, che appaiono di sicuro ausilio per la tutela della salute collettiva[9]. L'art. 5, paragrafo 1, lettere b) ed e), l'art. 9, paragrafo 2, lettera j), in combinato con le deroghe degli artt. 49 e 89 del GDPR, forniscono la base giuridica per il trattamento dei dati personali (relativi alla salute) a fini di ricerca scientifica, che può fare a meno del consenso dell'interessato per fondarsi su una norma di legge adottata dall'Unione o dai singoli Stati proporzionata allo scopo perseguito, rispettosa dell'essenza del diritto alla protezione dei dati e che preveda misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell' interessato.

La pandemia in atto rende indispensabile la raccolta di grandi quantità di informazioni, dirette alla creazione di banche dati aperte per gli studi sul monitoraggio dei focolai e sulle dinamiche del fenomeno, postulando una necessaria cooperazione internazionale che potrebbe comportare trasferimenti di dati relativi alla salute per finalità di ricerca scientifica al di fuori del territorio dell'Unione. Anche in questo caso la regolamentazione non fa difetto: quando i dati personali sono trasferiti verso un paese non appartenente al territorio europeo o verso un'organizzazione internazionale, oltre a rispettare le norme stabilite nel GDPR, in particolare gli artt. 5, 6 e 9, e quelle dettate dai singoli Stati, che potrebbero tuttavia differenziare tra loro, l'esportatore deve conformarsi anche alle norme del Cap V ("Trasferimento dei dati"). Tuttavia, come ha chiarito l'*European Data Protection Board* (EDPB) nelle *Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak* adottate il 21 aprile 2020, l'articolo 49 del RGPD prevede alcune situazioni specifiche in cui il trasferimento di dati personali può avvenire in via eccezionale: "Con riguardo all'attuale crisi dovuta al COVID-19, possono trovare applicazione le deroghe di cui all'articolo 49, paragrafo 1, lettera d) (trasferimento necessario per importanti motivi di interesse pubblico) e lettera a) (consenso esplicito)"[10].

Per usare le parole della presidente di questo organismo, Andrea Jelinek, il GDPR "is a broad legislation and also provides for the rules to apply to the processing of personal data in a context such as the one relating to Covid-19"[11].

3. Localizzazione e creazione di mappe epidemiologiche.

In aggiunta a quello appena descritto, le ripercussioni della regolamentazione dettata in tempi di Covid-19 sulla protezione dei dati personali e specificamente dei dati inerenti alla salute riguardano altri rilevanti aspetti. I profili che hanno maggiormente occupato gli studiosi e interessato l'opinione pubblica sono quelli che attengono all'impiego delle informazioni di localizzazione per delineare mappe epidemiologiche e all'uso degli strumenti di tracciamento dei contatti.

Al riguardo si impone una precisazione preliminare: le norme del GDPR vanno combinate con quelle della direttiva 2002/58/CE, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (c.d. direttiva *e-privacy*, che ad oggi, a causa di un interminabile processo di gestazione, non è ancora

l'evoluzione di epidemie e la loro diffusione o in casi di emergenze umanitarie in particolare in casi di catastrofi di origine naturale e umana".

[9] Ne costituiscono un chiaro esempio i dati necessari ad assicurare il monitoraggio del rischio sanitario di cui al d.p.c.m. del 26 aprile 2020 (allegato 10).

[10] Al trasferimento internazionale di dati per scopi di ricerca scientifica è dedicato in particolare il paragrafo 7 delle *Guidelines*, nel quale si legge che, nel contesto della eccezionale crisi sanitaria "non solo le autorità pubbliche, ma anche i soggetti privati che contribuiscono al perseguimento di tale interesse pubblico (ad esempio, un istituto di ricerca universitario che collabori alla messa a punto di un vaccino nell'ambito di un partenariato internazionale) potrebbero, nell'attuale contesto di pandemia, avvalersi della deroga di cui sopra. Inoltre, in determinate circostanze, in particolare quando i trasferimenti siano effettuati da soggetti privati per scopi di ricerca medica finalizzata a combattere la pandemia da COVID-19,28 tali trasferimenti di dati personali potrebbero avvenire in via alternativa sulla base del consenso esplicito degli interessati. Nel contesto dell'attuale pandemia, ove non sia possibile basarsi su una decisione di adeguatezza ai sensi dell'articolo 45, paragrafo 3, o su garanzie adeguate ai sensi dell'articolo 46, le autorità pubbliche e i soggetti privati possono ricorrere alle deroghe applicabili di cui sopra, principalmente come misura temporanea giustificata dall'urgenza della situazione sanitaria a livello mondiale".

[11] "Coronavirus: dichiarazione del 16 marzo 2020 del Comitato Europeo per la Protezione dei Dati".

riuscita a trasformarsi in regolamento), nel cui raggio applicativo rientrano tali tipologie di attività.

Come ha precisato l'EDPB, che, dopo una dichiarazione del 19 marzo 2020, il successivo 21 aprile ha emanato le attese *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*, i dati relativi all'ubicazione sono raccolti da fornitori di servizi di comunicazione elettronica (come gli operatori di telecomunicazioni mobili) nel corso della prestazione del loro servizio e da fornitori di servizi della società dell'informazione, la cui funzionalità richiede l'uso di tali dati (ad esempio, navigazione, servizi di trasporto, ecc.).

Questi dati possono essere trattati solo entro i limiti di cui agli articoli 6 e 9 della citata direttiva *e-privacy*, la quale prevede che i dati relativi alla geolocalizzazione e all'ubicazione (tratti dal traffico telefonico) possano essere utilizzati dall'operatore solo se resi anonimi o con il consenso dei singoli. L'articolo 15 della direttiva contempla la possibilità di introdurre misure legislative a tutela della sicurezza nazionale e pubblica, purché le stesse siano (Considerando 11) "*appropriate, strettamente proporzionate allo scopo perseguito, necessarie in una società democratica ed essere soggette ad idonee garanzie conformemente alla precitata Convenzione europea di salvaguardia dei diritti dell'uomo e delle libertà fondamentali*". Tali misure devono essere inoltre conformi alla Carta dei diritti fondamentali e alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali. Inoltre, esse sono soggette al controllo giurisdizionale della Corte di giustizia dell'Unione europea e della Corte europea dei diritti dell'uomo[12].

Di conseguenza, proprio con riferimento ai dati relativi all'ubicazione, l'EDPB ha precisato che occorre sempre privilegiare il trattamento di dati anonimi piuttosto che di dati personali, ma con un *caveat*, anzi due. Il primo è che i dati non possono essere resi anonimi isolatamente, il che significa che solo intere serie o interi insiemi di dati sono passibili di anonimizzazione. In tal senso, qualsiasi intervento su un dato isolato o sulla serie storica di dati riferibili a un singolo interessato (mediante cifratura o altre trasformazioni matematiche) può essere considerato, nel migliore dei casi, una pseudonimizzazione, con soggezione alla disciplina del GDPR. Il secondo è legato al fatto che approfondite ricerche hanno ormai dimostrato che i dati relativi all'ubicazione ritenuti anonimi possono di fatto non esserlo, per cui le "tracce di mobilità dei singoli individui sono caratterizzate intrinsecamente da forte correlazione e univocità [e] pertanto, in determinate circostanze, possono essere vulnerabili ai tentativi di re-identificazione". Da qui, la segnalata esigenza di utilizzare tecnologie "robuste" di anonimizzazione e di garantire la trasparenza per quanto attiene alla metodologia di anonimizzazione utilizzata.

Come tutte le situazioni che l'emergenza ha svelato nella loro essenzialità e spogliato di ogni orpello, l'uso dei *Big Data* presenta oggi in pieno il suo risvolto più squisitamente "politico". Come nel secolo breve la potenza di uno Stato è stata identificata nella capacità di controllare l'economia (o anche l'uso, mai sopito, della forza), ai tempi attuali questa capacità si misura con la possibilità di controllare i flussi di informazioni, divenuti elementi fondanti della c.d. economia delle piattaforme. Uno stato totalitario eseguirà questo controllo con metodi autoritari e per fini non resi noti; uno stato democratico dovrà farlo in modo trasparente, accessibile e condiviso.

4. I sistemi di *contact tracing* e la posizione delle Autorità garanti: l'approccio "pan-europeo".

Semplificando problematiche ben più complesse, lo scenario appena illustrato si è posto allo sfondo del dibattito sulla possibile trasposizione in Italia, ma anche nel contesto europeo, di modelli di contenimento del contagio che, con caratteristiche diverse, sono stata adottati dai primi Stati esposti alla pandemia: se il modello cinese è stato subito rigettato per il suo carattere fortemente pervasivo, generatore di rischi di discriminazione, i modelli della Corea democratica ma soprattutto, con maggior rilevanza, quello adottato dalla città-Stato di Singapore, hanno animato il confronto, specie tra i tecnologi, in vista della recente scelta italiana[13].

[12] Per queste ultime espressioni v. la dichiarazione dell'*European Data Protection Board* sul trattamento dei dati personali nell'epidemia di Covid-19 adottata il 19 marzo 2020.

[13] La Cina, in particolare, ha sviluppato ulteriormente il suo criticato sistema di sorveglianza con l'uso di 200 milioni di telecamere di sicurezza e di specifiche applicazioni per la creazione di *cluster* di *big data*, al fine di far rispettare la quarantena ai pazienti infetti e per mappare i movimenti dei potenziali infetti e quindi del virus, con scopi repressivi e di controllo. Ma non è solo l'estremo oriente a usare questo tipo di tecnologia. Di recente, il primo ministro israeliano ha autorizzato i servizi segreti interni a usare strumenti tecnologici di solito riservati alla lotta al terrorismo per seguire i malati di coronavirus. Il provvedimento non è stato prorogato in nome della necessaria difesa della privacy dei cittadini, in forza di un intervento della Corte suprema del 19 marzo 2020. Per una illustrazione del funzionamento di questi modelli cfr. N. MONTE-G. VACIAGO, Lotta al c*oronavirus, paese che vai privacy che trovi: i diversi approcci (Europa, Cina, Corea, Israele)*, in Agenda Digitale, 17 aprile 2020.

Tra vicende altalenanti e ripensamenti di alcuni Stati, come la Francia con il sistema StopCovid-19, in queste settimane si sta delineando, in Europa, quella che potrebbe essere chiamata "la via occidentale" all'uso governativo di grandi masse di dati e all'impiego di strumenti di *contact tracing*, sul presupposto, non del tutto dimostrato per vero, che l'impiego di questo tipo di tecnologia possa dare un contributo significativo al contenimento delle infezioni da Covid-19 ma che appaia comunque necessario approntare un "toolbox of practical measures", come dichiarato dalla Commissione europea nella raccomandazione UE 2020/518 rivolta l'8 aprile scorso agli Stati membri sull'uso della tecnologia e dei dati ai fini di contrasto alla pandemia.

La Commissione ha raccomandato l'adozione di un piano comune per l'utilizzo, in forma anonima e aggregata, dei dati relativi agli spostamenti della popolazione al fine di prevedere la diffusione del virus e l'andamento dell'epidemia e di un approccio "pan-europeo" per l'uso delle applicazioni mobili, guidati entrambi dal rispetto della tutela della vita privata e della protezione dei dati e volti ad attuare il monitoraggio della metodologia e la condivisione delle valutazioni dell'efficacia di tali applicazioni al fine di valutare l'adeguatezza dei processi decisionali delle istituzioni degli Stati membri. Per la Commissione è opportuno prevedere l'interoperabilità tra le applicazioni, al fine di evitare applicazioni di tracciamento dei contatti diverse tra persone che attraversano frontiere nazionali e di agevolare lo scambio di informazioni interoperabili sugli utenti positivi al test con altri Stati membri per affrontare le catene di trasmissione transfrontaliere, evitando approcci frammentati o non coordinabili.

Non stupisce, anche alla luce di queste premesse, che proprio l'uso delle applicazioni software (app) di *contact tracing* da installare sullo *smartphone* sia stato al centro di un particolare interessamento. L'impiego dell'app può aiutare a identificare individui potenzialmente infetti prima che emergano sintomi e può contribuire ad impedire la trasmissione successiva dai casi secondari, supplendo, con l'aiuto dei dati telefonici, alle carenze della memoria della persona rivelatasi poi contagiata nel ricostruire i suoi precedenti spostamenti e, dunque, i possibili contatti. Queste applicazioni possono quindi rivestire, come indicato dalla Commissione, "un ruolo importante nel tracciamento dei contatti, limitando la propagazione della malattia e interrompendo le catene di trasmissione".

I requisiti di conformità alla normativa sulla protezione dei dati personali che deve presentare l'uso di tali applicativi sono stati nitidamente tracciati, prima della scelta poi compiuta dal Governo del nostro Paese, della quale si dirà, dalle autorità garanti, con l'avvertenza che le indicazioni formulate dal Garante Privacy italiano sull'uso delle tecnologie e della rete per contrastare l'emergenza epidemiologica hanno in parte anticipato quelle poi provenute dall'EDPB.

La prima condizione è rappresentata dall'esigenza di non operare un uso isolato dell'app ma di inserire il suo funzionamento all'interno in un sistema composito e integrato di sanità pubblica, nel quale devono essere presenti componenti non tecnologiche. In altri termini, il funzionamento dell'app deve essere seguito da altri strumenti, come i test diagnostici e soprattutto da interventi di operatori del sistema sanitario, anche per consentire la tracciabilità manuale dei contatti al fine di eliminare i casi dubbi ("*subsequent manual contact tracing for the purpose of doubt removal*")[14]. In questo modo si eviterebbe la soggezione a decisioni esclusivamente automatizzate, interamente affidate all'algoritmo, come richiesto dall'art. 22 del GDPR, consentendo la correzione di possibili imprecisioni e storture, dal rilevante impatto sulla salute e sulla libertà dei singoli, dovute all'impiego di informazioni inesatte.

Il secondo, imprescindibile requisito è l'esclusione di ogni obbligatorietà nell'utilizzo dell'app: l'obbligatorietà striderebbe con il principio di proporzionalità dell'uso delle informazioni, porrebbe problemi di coercibilità (come imporre ai cittadini di non uscire di casa senza lo *smartphone*) e per una certa parte della popolazione significherebbe anche obbligatorietà dell'acquisto del dispositivo sul quale fare funzionare l'applicazione.

Le Linee Guida dell'EDPB chiariscono le condizioni e i principi per "l'uso proporzionato" degli strumenti di tracciamento dei contatti, sul presupposto dichiarato che il monitoraggio su larga scala della localizzazione o dei contatti tra le persone rappresenta una grave intrusione della sfera privata delle persone, che può essere legittimata solo in base alla volontaria adozione da parte dell'utente per la specifica finalità.

Dal rispetto del principio di minimizzazione del trattamento dei dati personali sono derivate una serie di raccomandazioni. Anzitutto, la constatata sovrabbondanza dei dati forniti da dispositivi di geolocalizzazione: su questo presupposto, ossia sulla sufficienza allo scopo di un dato di "contatto" (*proximity data,* come l'identificativo *blue-*

[14] L'EDPB ha evidenziato, in particolare, il problema dei falsi, in quanto la raccolta automatizzata comporterà sempre, in una certa misura, la possibilità del verificarsi di falsi positivi. Poiché l'identificazione di un rischio di infezione può avere un forte impatto sui singoli individui, ad esempio imponendo l'autoisolamento fino a negativizzazione del test, è indispensabile poter effettuare, con l'impiego dell'uomo, correzioni dei dati e/o dei risultati delle analisi successive.

tooth), la scelta si è diretta verso quest'ultima tecnologia in luogo di quella GPS, che traccia gli spostamenti delle persone. Secondariamente, la necessità di trattare dati in forma anonima o almeno pseudonima[15]. Infine, un uso limitato dell'opera di "personalizzazione" dei dati nella fase successiva alla raccolta, in vista del loro utilizzo per allertare i potenziali contagiati, nel senso che questa dovrebbe avvenire limitatamente ai soggetti risultati poi positivi e a coloro ai quali siano entrati con essi in contatto significativo per il solo periodo di potenziale contagiosità.

Fermo restando che l'uso della app deve essere volontario, dunque rimesso al consenso dell'interessato[16], per l'EDPB la condizione di liceità del trattamento va ravvisata nell'esecuzione di un compito di interesse pubblico di cui all'art. 6, par. 1 lett. e) del GDPR[17]. Secondo l'art. 6 par. 3, questa base giuridica deve essere stabilita dal diritto dell'Unione o dello Stato membro: per questa ragione, l'impiego della app per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento deve essere previsto per legge.

La "compliance" alla normativa sulla protezione dei dati personali si completa con la sottolineata esigenza di vincolare la durata del trattamento al solo periodo dell'emergenza e con la necessità di effettuare una valutazione d'impatto[18] sulla protezione dei dati prima di implementare le app in questione, raccomandata sia dal Garante italiano sia dall'EDPB, in quanto il trattamento configura una probabilità di rischio elevato (dati relativi alla salute, adozione prevista su larga scala, monitoraggio sistematico, uso di una nuova soluzione tecnologica). Il Comitato raccomanda vivamente anche la pubblicazione degli esiti di tali valutazioni.

I criteri di necessità, proporzionalità e minimizzazione rimarcati dalla giurisprudenza europea indicano, dunque, l'esigenza di contenere l'utilizzo dei dati inerenti alla salute nella misura strettamente necessaria a perseguire fini rilevanti, nella specie di tipo solidaristico, con il minor sacrificio possibile per gli interessati, in un arco temporale di riduzione delle garanzie esattamente delimitato.

5. La scelta italiana della app "Immuni" e il d. l. n. 28/2020.

Dopo una selezione che ha visto coinvolta la *task force* nominata dal Ministero dell'Innovazione, il Commissario straordinario per l'emergenza epidemiologica da Covid-19 ha scelto a tale scopo la app di tracciamento denominata "Immuni", che ricorre alla tecnologia *bluetooth-low-energy* per inviare *alert* agli *smartphone*, utilizzando solo nel momento in cui un individuo viene trovato infetto a seguito di test diagnostico i dati di prossimità presenti sul suo terminale[19].

L'impiego della app è stato legittimato dall'art. 6 del decreto 29 aprile 2020 n. 28, che non usa mai la parola "tracciamento", nemmeno nella sua rubrica ("Sistema di allerta Covid-19") e che non fa menzione neppure della app "Immuni" individuata, tra oltre trecento presentate in risposta alla *call* del Ministero dell'Innovazione, dal Commissario straordinario. Questa norma, che costituisce la base giuridica dell'uso della app di allerta, ne ha scolpito le caratteristiche e ha stabilito le garanzie per il trattamento dei dati con essa raccolti, con la precisazione, inserita nelle righe di apertura, che l'uso dell'app avverrà su base volontaria e che il mancato utilizzo non avrà conseguenze o limiti riguardo "all'esercizio dei diritti fondamentali dei soggetti interessati".

Questi, in sintesi, i requisiti che dovrà avere l'applicazione.

Sarà approntata anzitutto una piattaforma unica nazionale per la gestione del sistema di allerta, di titolarità pubblica e utilizza esclusivamente con infrastrutture localizzate sul territorio nazionale e gestite da soggetti pubblici o società a totale

---

[15] Si ricorda però che solo i dati anonimi esulano dal campo di applicazione del GDPR, mentre quelli pseudonimi, in quanto capaci di tornare a rivelare le informazioni personali (cfr. la definizione di pseudonimizzazione contenuta nell'art. 4, comma 1, n. 5 del GDPR) sono ad esso sottoposti. Sul punto cfr., ad esempio, *Codice della disciplina* privacy, Commentario diretto da L. Bolognini e E. Pelino, Milano, 2019, p. 40 ss. V. anche, sullo specifico aspetto, *infra*, nota 21.

[16] Il Garante privacy è esplicito nel sottolineare che il consenso all'uso della app deve essere libero e non condizionato alla fruizione di determinati servizi o beni: v. *Audizione informale, in videoconferenza, del Presidente del Garante per la protezione dei dati personali sull'uso delle nuove tecnologie e della rete per contrastare l'emergenza epidemiologica da Coronavirus* avanti alla Commissione IX (Trasporti, Poste e Telecomunicazioni) della Camera dei Deputati dell'8 aprile 2020.

[17] "*Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: ... e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento*". Sulle condizioni di liceità del trattamento, in generale, cfr. F. BRAVO, *Le condizioni di liceità del trattamento dei dati personali*, in *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, a cura di G. Finocchiaro, Bologna, 2019, p. 110 ss.

[18] Sulla quale cfr. A. MANTELERO, *Il nuovo approccio della valutazione del rischio nella sicurezza dei dati. Valutazione d'impatto e consultazione preventiva* (artt. 32-39), in *Il nuovo regolamento europeo sulla* privacy *e sui dati personali*, a cura di G. Finocchiaro, Bologna, 2017, p. 287 ss.

[19] Per un'illustrazione del funzionamento della app v. G. ATTARDI-N. MARINO-E. SANTUS, Contact tracing, *perchè è così importante contro il covid (anche in Italia)*, in Agenda digitale, 17 aprile 2020.

partecipazione pubblica. Il titolare del trattamento è individuato nel Ministero della salute, il quale "si coordinerà", come si legge nel comma 1, con tutta una serie di altri soggetti, a partire dai soggetti operanti nel servizio nazionale della Protezione Civile (i quali potranno assumere, in forza del rinvio operato dalla norma all'art. 28 GDPR, la veste di responsabili del trattamento).

Prima di attivare l'app gli utenti dovranno ricevere adeguata informativa circa le finalità e le operazioni di trattamento, le tecniche di pseudonimizzazione utilizzate e i tempi di conservazione dei dati. Potranno essere raccolti solo dati necessari ad avvisare gli utenti che si siano trovati a stretto contatto di altri utenti accertati positivi al Covid-19 e ad agevolare l'eventuale adozione di misure di assistenza sanitaria in loro favore; i dati raccolti non potranno essere trattati per finalità diverse da quella indicate, salvo l'utilizzo in forma aggregata o comunque anonima, per soli fini di sanità pubblica, profilassi, finalità statistiche o di ricerca scientifica; i dati di prossimità dei dispositivi saranno resi anonimi o, se non è possibile, pseudonimizzati; la conservazione dei dati relativi ai contatti, anche nei cellulari, sarà limitata al tempo strettamente necessario; l'utilizzo dell'applicazione e della piattaforma e i trattamenti dei dati personali saranno interrotti nel momento in cui sarà decretata la cessazione dello stato di emergenza e comunque non oltre il 31 dicembre 2020; entro la medesima data saranno cancellati o resi definitivamente anonimi tutti i dati personali trattati.

Si legge nel decreto che i programmi informatici sviluppati per la realizzazione della piattaforma e dell'applicazione sono resi disponibili e rilasciati con licenza aperta. Emerge dunque il ruolo dell'*open source* per garantire la trasparenza, come richiesto dallo stesso Parlamento europeo con la risoluzione del 17 aprile 2020[20]. A questo scopo soccorre anche la giusta declinazione del principio di *privacy by design* di cui all'art. 25 del GDPR, che è alla base di quanto stabilito nel comma 2, lettera b): per impostazione predefinita, i dati personali raccolti dall'applicazione saranno solo quelli necessari ad avvisare gli utenti di essere rientrati "tra i contatti stretti di altri utenti risultati positivi al Covid-19", così da garantire la proporzionalità tra i dati impiegati e le finalità del trattamento.

6. *Segue*. Centralizzazione o delocalizzazione della raccolta dei dati?

La prima lettura del testo solleva qualche rilievo sul tema dell'anonimato[21], che coinvolge anche il profilo del riuso[22] e può evidenziare che in esso non si fa alcun riferimento al tema dell'interoperabilità auspicato dall'approccio "pan-europeo". Soprattutto, non è chiarito il collegamento dell'uso della app con gli interventi di assistenza sanitaria, in modo da realizzare quel sistema integrato ritenuto indispensabile dalle autorità garanti europee ed italiana per un efficace funzionamento del dispositivo.

Dal d.l. n. 28/2020 si desume inoltre che la piattaforma unica nazionale dialogherà con la app di

[20] Il Parlamento europeo ha invitato la Commissione e gli Stati membri "a pubblicare i dettagli di tali sistemi e a consentire il controllo pubblico e la completa sorveglianza da parte delle autorità preposte alla protezione dei dati".
Nell'ordinanza 10/2020 del Commissario straordinario per l'emergenza Covid-19 per la stipulazione del contratto di concessione gratuita del *software* di *contact tracing* si legge: *"Bending Spoons (id est, la società produttrice della app) ha concesso la licenza d'uso aperta, gratuita, perpetua e irrevocabile del codice sorgente e di tutte le componenti dell'app "Immuni", nonché si è impegnata, sempre gratuitamente e pro bono, a completare gli sviluppi software necessari per la messa in esercizio del sistema nazionale di contact tracing digitale, per la durata di sei mesi e comunque nel limite di 10.000 ore/uomo"*. La app risulterebbe conforme al modello europeo delineato dal Consorzio PEPP-PT (*Pan-European Privacy-Preserving Proximity Tracing)*, realizzato da un gruppo di 130 scienziati e più di trenta aziende e istituti di ricerca di otto Paesi.
Per rilievi critici sulla procedura adottata per la scelta di "Immuni" cfr. P. Clarizia-E. Schneider, *Luci e ombre sulla procedura di selezione di "Immuni", l'app del governo di tracciamento del contagio da Covid-19, in* www.irpa.eu, *Osservatorio sullo stato digitale*, 19 aprile 2020.

[21] Di fronte alla necessità di utilizzare il più possibile dati non personali si pone la previsione dell'art. 6, comma 2, lettera c), secondo la quale il trattamento di allerta è basato sui "dati di prossimità dei dispositivi, resi anonimi oppure, *ove ciò non sia possibile* (corsivo aggiunto, n.d.a.), pseudonimizzati" (da qui, la conseguenza che l'informativa debba contenere le indicazioni sulle tecniche di pseudonimizzazione), anche se la possibilità di usare sistemi di pseudonimizzazione o di cifratura è stata adombrata dalle autorità garanti che, come si è visto (*supra*, § 3), avanzano dubbi sulla possibilità di garanzia di una anonimizzazione sicura. La valutazione di impatto dovrebbe essere utile a prevedere anzitutto a questo proposito le scelte più opportune e le misure "adeguate ad evitare il rischio di reidentificazione degli interessati cui si riferiscono i dati pseudonimizzati oggetto di trattamento" (art. 6, comma 2, lettera e).

[22] Il terzo comma della norma in commento fa salva la possibilità di utilizzo dei dati "in forma aggregata o comunque anonima" anche per finalità diverse ma riconducibili "a fini di sanità pubblica, profilassi, statistici o di ricerca scientifica", in conformità agli artt. 5, par. 1, lettera a) e 9, par. 2, lettera i e j). Non sussiste però identità tra la forma aggregata e la forma anonima e potrebbe emergere anche l'esigenza di continuare ad utilizzare *full-personal-data* per seguire al meglio il paziente e la cerchia dei suoi familiari con la medicina di precisione nel corso del tempo.
Evidenzia come non sia difficile immaginare "che anche il *lockdown,* con l'estensivo impiego 'domiciliare' delle piattaforme e dei social rappresenti una ghiotta occasione per l'industria dei dati personali", R. D'Orazio, *La* privacy *ai tempi del Covid-19*, in *Il mondo degli archivi*, 31 marzo 2020.

contact tracing, ma l'art. 6, comma 2, lettera e) prevede altresì che "*i dati relativi ai contatti stretti siano conservati anche nei dispositivi mobili degli utenti*" per il periodo strettamente necessario al trattamento, la cui "*durata è stabilita dal Ministero della salute*".

Non è del tutto chiaro se si adotterà nel rapporto tra app e piattaforma pubblica un sistema centralizzato o decentralizzato, profilo, questo, che ha polarizzato la discussione delle scorse settimane[23].

L'EDPB e anche il Garante italiano si sono pronunziati in favore dell'adozione di un sistema decentralizzato, considerato più rispettoso della normativa in tema di *Data Protection*[24]. Anche la risoluzione del parlamento europeo del 17 aprile 2020, appena citata, va in questa direzione[25]. Un sistema decentralizzato è quello sul quale stanno lavorando Apple e Google, che hanno di recente stretto un'inedita alleanza per aiutare le agenzie sanitarie pubbliche a ridurre la diffusione del contagio, facilitando l'uso della tecnologia *bluetooth* su un'ampia gamma di dispositivi mobili.

Un sistema centralizzato accentra il trattamento sotto la direzione di un'autorità pubblica, che può identificare gli individui che sono stati a contatto con il soggetto positivo e prevede un server appunto centrale, una banca dati centralizzata nella quale immagazzinare i dati; un sistema decentralizzato si limita invece ad inviare a tutti i dispositivi degli utenti del sistema stesso l'elenco dei contatti dell'identificativo anonimo corrispondente al soggetto risultato positivo. A questo punto, l'app sul dispositivo confronterà questo elenco di contatti anonimi e se un codice corrisponde con il proprio, lo notificherà al titolare del dispositivo: l'operazione, pertanto, è svolta dall'app del dispositivo e non dal server, come, invece, accade nel modello centralizzato. Di conseguenza solo la persona a cui arriva l'alert saprà di avere avuto un contatto con un soggetto positivo, senza conoscere la sua identità.

Nel sistema decentralizzato solo il singolo è a conoscenza del contatto con il soggetto positivo (nel sistema centralizzato, invece, anche chi ha accesso ai dati del server conosce il dato relativo al numero dei contatti tra persone contagiate e sane); di conseguenza il sistema fa completamente leva sulla "responsabilizzazione" del singolo, ossia sul fatto che, una volta saputo di essere stato a contatto con un soggetto positivo, questi agisca di conseguenza.

Il primo, a differenza del secondo, è meno sicuro e più vulnerabile dal punto di vista di possibili attacchi esterni e richiede uno sforzo di protezione del server centrale. Oltre che da questo punto di vista, non pare che le due soluzioni siano indifferenti neppure dal punto di vista della individuazione del titolare del trattamento, posto che il mantenimento dei dati sul terminale dell'utente è un tipo di attività che rientra tra quelle normate dall'articolo 5, par. 3, della direttiva *e-privacy*[26].

Si è privi di competenze specifiche per approfondire ulteriormente il problema, ma si può ricordare che anche su questo profilo il Garante privacy ha avuto modo di suggerire che sul server vadano "raccolti solo gli identificatori pseudonimi dell'utente diagnosticato come infetto a seguito di un controllo delle autorità sanitarie, oppure, in alternativa, sul server potranno essere caricati una lista di identificatori pseudonimi degli utenti infetti o dei loro contatti ma solo per il tempo necessario per informare i potenziali soggetti a rischio di esposizione"[27].

---

[23] Da notare che il parere della task force sulla app "Immuni" dichiara che per la parte server viene utilizzata la piattaforma *Google Cloud Platform*. La relazione (Gruppo di lavoro 8- Profili giuridici, Relazione proposta n. 100) si può consultare sul sito https://innovazione.gov.it/task-force-dati-le-relazioni-delle-attivita-dei-gruppi-che-hanno-valutato-le-app/.

[24] Secondo il Garante italiano "sarebbero apprezzabili quelle tecnologie che mantengono il diario dei contatti esclusivamente nella disponibilità dell'utente, sul suo dispositivo, ragionevolmente per il solo periodo massimo di potenziale incubazione".

[25] Il Parlamento chiede, tra l'altro, "che la memorizzazione dei dati sia completamente decentralizzata, che vi sia piena trasparenza sugli interessi commerciali (extra UE) degli sviluppatori di queste applicazioni e che siano fornite chiare proiezioni a dimostrazione del fatto che l'uso di applicazioni per la ricerca dei contatti da parte di una fetta della popolazione, in combinazione con altre misure specifiche, porterà a un numero significativamente inferiore di contagi".

[26] Il quale, dedicato alla "*Riservatezza delle comunicazioni*", precisa che "*Gli Stati membri assicurano che l'uso di reti di comunicazione elettronica per archiviare informazioni o per avere accesso a informazioni archiviate nell'apparecchio terminale di un abbonato o di un utente sia consentito unicamente a condizione che l'abbonato o l'utente interessato sia stato informato in modo chiaro e completo, tra l'altro, sugli scopi del trattamento in conformità della direttiva 95/46/CE e che gli sia offerta la possibilità di rifiutare tale trattamento da parte del responsabile del trattamento*". Sicuramente il trattamento in questione non rientra nell'esenzione della memorizzazione tecnica al fine di effettuare o facilitare la comunicazione prevista nella stessa norma.

[27] L'operatività dei sistemi di *contact tracing*, secondo criteri rispondenti alla normativa sul trattamento dei dati personali, è stato puntualmente illustrato dal Garante privacy nella citata *Audizione informale, in videoconferenza, del Presidente del Garante per la protezione dei dati personali sull'uso delle nuove tecnologie e della rete per contrastare l'emergenza epidemiologica da Coronavirus* avanti alla Commissione IX (Trasporti, Poste e Telecomunicazioni) della Camera dei Deputati dell'8 aprile 2020: "Il soggetto che risultasse positivo dovrebbe fornire l'identificativo Imei del proprio dispositivo all'asl, che sarebbe poi tenuta a trasmetterlo al server centrale per consentirgli così di ricostruire, tramite un calcolo algoritmico, i contatti tenuti con altre persone le quali si siano, parimenti, avvalse

7. Una app ci salverà?

Gli effetti dell'operatività della soluzione accolta sono rimessi alla sua inevitabile sperimentazione[28], ma alcuni risvolti possono fin d'ora essere analizzati.

Si è già detto che, specie dietro le sollecitazioni dei Garanti, il suo funzionamento deve essere inserito in un contesto di reazioni da parte delle autorità sanitarie e di scelte epidemiologiche, che postula il necessario l'intervento di un operatore, nel momento la fase che segue l'invio automatico del "warming". Questa fase è oltremodo delicata, sia perché è con riguardo ad essa che si reidentifica il destinatario, e quindi i suoi dati, non più associati a una sequenza di numeri, tornano "in chiaro", sia perché si deve evitare la creazione di uno "status" di possibile contagiato, che dovrebbe postulare un accesso in tempi brevi ai test diagnostici. In assenza di tutto ciò, il rischio di limitare i diritti del cittadino che poi risulta non infetto risulterebbero elevati.

A complicare ulteriormente il contesto soccorrono altre considerazioni, che attengono al problema degli incentivi all'uso della app di allerta Covid-19.

La app riuscirà a soddisfare l'intento per cui il Governo ne ha propugnato l'utilizzo quando ad utilizzarla sarà una fetta consistente della popolazione. Tutto questo dipenderà dal grado di penetrazione del suo impiego, che potrebbe essere motivato sia da fini egoistici (sapere di avere corso il rischio di contagio) sia da finalità altruistiche (evitare l'ulteriore diffusione ad altri del virus), nonché dalla capacità di affermarsi come unica app di tracciamento[29]. Sarà particolarmente rilevante, in questa direzione, la forza della comunicazione e il grado di persuasione di campagne informative per l'adesione volontaria, e il suo allontanamento da impieghi stigmatizzanti: si percepisce invero un certo timore al rilascio di informazioni tramite l'uso di questo strumento, mentre finora non si sono mai avute remore, ad esempio, all'uso di braccialetti *fitness*, ricettacolo di informazioni spesso sensibili.

La mancanza di obbligatorietà può essere sostituita solo dalla fiducia nell'uso della applicazione e la fiducia aumenta solo se si garantisce ai cittadini un trattamento corretto e trasparente dei dati, oltre che l'immunità da conseguenze pregiudizievoli in caso di non utilizzo della stessa.

Precisato che il mancato uso non può generare effetti negativi di sorta, pena non solo la mancata installazione ma anche l'abbandono volontario e momentaneo del dispositivo, si pone, come si anticipava, la questione dell'impiego di incentivi. Se l'utilizzo di questo sistema fosse prefigurato come un presupposto necessario per fruire di certi servizi, la conseguenza sarebbe, a ben vedere, la trasformazione di un consenso libero alla sua installazione in un consenso condizionato e non valido ai sensi del GDPR. La previsione che un soggetto "allertato" abbia la precedenza su uno non "allertato" nell'accesso al sistema di protezione sanitaria, specie in un periodo di numero contingentato di tamponi, altererebbe invece quella parità di trattamento che la norma che ne prevede l'applicazione (art. 6 comma 4° del citato d.l. 30 aprile 2020, n. 28) intende assicurare, tanto che sono già stati prospettati taluni dubbi sul piano della costituzionalità di tutto il sistema[30].

Ma alcuni rilievi soccorrono anche sotto il profilo dell'efficienza. Gli esperti hanno dichiarato che per un ottimale funzionamento l'applicazione dovrebbe essere utilizzata dal 60% della popolazione. Dando per buono questo dato, si deve osservare che nel nostro Paese gli *smarthphone* non risulterebbero diffusi in tale quantità e non è difficile ipotizzare che tali dispositivi non siano usati proprio nella fascia della popolazione più anziana e dunque a maggior esposizione al rischio. Inoltre, secondo l'ultimo rapporto Desi[31], solo il 44% della popolazione italiana tra i 16 e i 74 anni possiede competenze digitali di base a fronte della media europea del 57%.

dell'app *blue tooth*. Queste ultime riceverebbero poi una segnalazione (nella forma di un *alert* sul sistema) di potenziale contagio, con l'invito a sottoporsi ad accertamenti che, naturalmente, sarà efficace nella misura in cui sia responsabilmente seguito. In tal modo, il tracciamento sarebbe affidato a un flusso di dati pseudonimizzati, suscettibili di reidentificazione solo in caso di rilevata positività. Anche in tali circostanze, comunque, la stessa comunicazione tra server centrale ed app dei potenziali contagiati avverrebbe senza consentirne la reidentificazione, così minimizzando l'impatto della misura sulla privacy individuale. In alternativa all'*alert* intra-app, si potrebbe ipotizzare che sia direttamente l'asl ad avvisare e, quindi, sottoporre ad accertamento le persone le quali, dalle rilevazioni *bluetooth*, risultino essere entrate in contatto significativo con il soggetto positivo".

[28] Le cronache riportano una certa oscillazione della struttura della app "Immuni", che sarebbe trascorsa dall'uno all'altro metodo (centralizzato/decentralizzato). Comunque, la app non risulta ancora ad oggi disponibile.

[29] Apple e Google hanno rivelato l'intenzione di apportare modifiche ai rispettivi sistemi operativi e includere una loro app di tracciamento nelle versioni rilasciate a partire dall'anno prossimo. Ci si potrebbe domandare quale sarà il rapporto tra queste app e l'app di tracciamento governativa e se le app dei due giganti del Web comunicheranno con i server delle autorità sanitarie.

[30] Non a caso gli studiosi costituzionalisti hanno già cominciato ad evidenziare dubbi di legittimità costituzionale: A. CELOTTO, "*Immuni" e la Costituzione*, in *Giustizia civile.com*, Editoriali, 29.04.2020.

[31] Indice di digitalizzazione dell'economia e della società- Relazione nazionale per il 2019.

Poiché l'app funziona tanto meglio quanto è impiegata da fasce ampie di popolazione, ma sarà più diffusa dove più elevato è il possesso di cellulari con *bluetooth* e il grado di alfabetizzazione digitale, non è così remoto il rischio di generare risvolti iniqui e di rafforzare il divario digitale, nella forma del *digital divide* cognitivo.

8. Incertezze del futuro, fermezza del diritto e problemi etici.

L'emergenza sanitaria ha segnato improvvisamente il passaggio ad una inaspettata fase di controllo, fino a pochi mesi fa riservata solo a determinate categorie di soggetti, con accertamenti e verifiche sulle strade e persino dal cielo tramite l'uso dei droni, ma, soprattutto, con la nostra quotidianità scandagliata e indirizzata nelle sue abitudini consolidate e persino nelle più elementari attività (fare la spesa, passeggiare, uscire per andare al lavoro, a scuola, al parco, a trovare familiari e amici, partecipare a un corteo funebre e molto altro).

Durante la "fase 2", quella del graduale ritorno alla normalità dopo il *lockdown*, le misure di emergenza adottate e l'uso delle app di tracciamento ci permetteranno probabilmente di verificare l'utilità del "capitalismo della sorveglianza"– per ricorrere alla ormai celebre espressione coniata da Shoshana Zuboff[32] – per la tutela della salute pubblica. Per il sociologo bielorusso Evgeny Morozov, forse il più critico detrattore di una certa gestione dell'ecosistema digitale, l'idea di costruire un nuovo ordine sulle fondamenta digitali offerte dai giganti della Rete o dagli operatori di telefonia mobile dei diversi paesi non produrrà "niente di buono: sarà, nel migliore dei casi, l'ennesimo parco giochi per soluzionisti; nel peggiore, una società totalitaria fondata proprio sul controllo e sulla sorveglianza diffusi".

Senza arrivare a questo pessimismo, che pure ha trovato reali preoccupanti conferme in svolte assolutistiche che in Europa sono state agevolate dallo sfruttamento dello stato di emergenza sanitaria, si deve prendere atto che l'attuale momento ha innescato, anche nei paesi non totalitari, un processo di inevitabile torsione dei diritti fondamentali. Non vi è dubbio che il diritto alla protezione dei dati personali appartenga a questa categoria, come previsto dall'art. 8 della Carta dei diritti fondamentali dell'UE, e che per esso il bilanciamento con esigenze prioritarie, anzitutto con la tutela della salute pubblica, anche in tempi mai vissuti come quelli odierni, debba essere svolto con grande accortezza.

Parole come adeguatezza e proporzionalità delle misure di trattamento dei dati personali, rimarcate anche dalla giurisprudenza europea, unite al principio-cardine del rispetto della dignità dei malati e dei loro familiari, devono guidare necessariamente questo percorso e devono orientare il legislatore in primo luogo, ma anche interpreti, scienziati, medici, operatori, programmatori, sviluppatori; insomma tutti gli attori della scena. Un trattamento indiscriminato, lontano dalle coordinate tracciate dal GDPR giustificato dall'emergenza rischia di avere conseguenze pregiudizievoli anche nella fase post-emergenziale.

In questa fase di cambiamento epocale, anche i giuristi sono chiamati a un grande impegno: tutt'altro che silenti[33], non solo stanno apportando, anche se senza clamori, un importante contributo al dibattito, come comprovano i numerosi interventi già editi[34], ma, soprattutto, avvezzi a ragionare oltre il contingente, stanno già riflettendo sulla "nuova normalità" che si prospetterà per la fase successiva all'emergenza Coronavirus e sulla capacità del diritto dell'oggi di governare i rapporti personali e patrimoniali del presente e del futuro.

Se sarà doveroso prendere atto dell'innesco di un irreversibile processo di digitalizzazione, sarà altrettanto necessario non cedere alla tentazione di affidare interamente alla tecnologia la risoluzione dei problemi. Probabilmente stiamo chiedendo a tecnologie non del tutto mature o non sufficientemente sperimentate di reagire molto velocemente a situazioni permeate di grande incertezza e di difficile previsione nel loro successivo andamento, a fronte di decisioni che, fino a un paio di mesi fa, sarebbero state assunte in tempi meno frenetici.

[32] Le teorie di Shoshana Zuboff, espresse nel libro tradotto in italiano con il titolo il "*Capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*" (Luiss University Press, 2019) hanno destato grande interesse. L'autrice definisce il processo di "estrazione del surplus comportamentale" dai dati capitalismo estrattivo, che appartiene alla «terza modernità», nella quale la logica economica è subordinata a un nuovo contesto che prevede la trasformazione comportamentale della popolazione.

[33] Il filosofo Agamben, tra i più strenui "negazionisti" dell'epidemia, in un articolo che ha destato vivaci reazioni (G. AGAMBEN, *Una domanda*, in *Quodlibet*, 13 aprile 2020), ha accusato i giuristi di avere abdicato ai loro compiti (l'accusa rivolta ai giuristi riguarda nello specifico il silenzio verso la decretazione emergenziale riguardo alle limitazioni della libertà personale).

[34] Per le riflessioni di matrice civilistica e lavoristica cfr. i vari contributi pubblicati in *Giustizia civile.com*, Emergenza Covid-19 -Speciale, n. 1/2020. E cfr. G. VETTORI, *Persona e mercato ai tempi della pandemia*, in *questa Rivista*, 2020, p. 3 ss., nonché G. GRISI, *La lezione del Coronavirus*, in *Jus Civile*, 2020, p. 190 ss. e A. M. BENEDETTI, *Il rapporto obbligatorio al tempo dell'isolamento: brevi note sul Decreto "Cura Italia"*, in *I contratti,* 2020, 231 ss. V. anche l'Osservatorio Emergenza Covid-19 della rivista *Federalismi.it* e della rivista *Astrid on line*.

In questo momento storico diviene ancora più indispensabile rafforzare ulteriormente il dialogo tra diritto e tecnica per non affidare unicamente alla seconda poteri salvifici ma per assumere decisioni sorrette da grande ponderatezza, equilibrio e anche lungimiranza, al fine di non rischiare che ciò che ci pare eccezionale oggi possa considerarsi normale domani.

L'angolatura dell'emergenza considerata in questo contributo mostra chiaramente che il potere pubblico ha necessità di spronare, per arginare un flagello così devastante, l'assunzione di contegni individuali. Tutto ciò accosta alla questione giuridica una questione etica di particolare rilievo. Solo con comportamenti che ciascuno può responsabilmente assumere in nome della sua appartenenza a una comunità e al rispetto della salute di familiari, conoscenti ma anche perfetti estranei, si potrà dare un forte contributo all'uscita dall'emergenza.

Pur essendo opportuno distinguere "obbedienza" e "responsabilità individuale" (la prima "cosa giuridica", la seconda "cosa etica"[35]), va posto nella debita luce e valorizzato nel suo senso più autentico il ruolo del dovere di solidarietà sociale. Proprio la solidarietà, che specifica anche il rapporto tra tutela della salute individuale e protezione della salute collettiva dell'art. 32 Cost., permette di assegnare un fondamento giuridico alle scelte individuali, che si scoprono (o si riscoprono) poste all'interno di una rete di rapporti strettamente interconnessi, e non solo virtualmente.

Non sarà dunque una app a salvarci, ma solo l'assunzione di comportamenti responsabili sollecitati (in certo qual modo "imposti"[36]) dall'esigenza di preservare non solo egoisticamente la nostra incolumità ma, altruisticamente, anche quella degli appartenenti alla nostra comunità.

[35] É l'opinione di Gustavo Zagrebelsky nell'articolo ("L'obbedienza e la responsabilità") apparso su La repubblica del 30 aprile 2020.

[36] "La solidarietà non è un concetto, ma una norma che fonda precisi doveri di condotta", nel senso che "esige, ad ogni livello, l'attuazione di quel principio attraverso l'indicazione di "comportamenti dinamici che devono essere tenuti da soggetti pubblici e privati": in questi termini si esprime G. VETTORI, *Persona e mercato al tempo della pandemia*, cit., p. 6.