GIUSTIZIA CIVILE.com

LA PROTEZIONE DEI DATI PERSONALI NEL DIRITTO DELL'EMERGENZA COVID-19

di **GIORGIO RESTA**

Editoriale del 05 maggio 2020

ISSN 2420-9651

Le misure giuridiche adottate negli ultimi mesi, nel nostro e in altri ordinamenti giuridici (si v., ad es.,, in Germania, il recente "pacchetto" normativo composto dal Gesetz zum Schutz der Bevölkerung bei einer epidemischen Lage von nationaler Tragweite e dal Gesetz zur Abmilderung der Folgen der COVID-19-Pandemie im Zivil-, Insolvenz- und Strafverfahrensrecht, entrambi del 27 marzo 2020), per mitigare e contenere gli effetti dell'epidemia da coronavirus toccano trasversalmente molteplici settori del diritto interno, dal diritto dell'economia al diritto tributario, dal diritto del lavoro al diritto amministrativo.

1. Le risposte giuridiche all'emergenza sanitaria: introduzione.

Le misure giuridiche adottate negli ultimi mesi, nel nostro e in altri ordinamenti giuridici (si v., ad es.,, in Germania, il recente "pacchetto" normativo composto dal *Gesetz zum Schutz der Bevölkerung bei einer epidemischen Lage von nationaler Tragweite* e dal *Gesetz zur Abmilderung der Folgen der COVID-19-Pandemie im Zivil-, Insolvenz- und Strafverfahrensrecht,* entrambidel 27 marzo 2020), per mitigare e contenere gli effetti dell'epidemia da coronavirus toccano trasversalmente molteplici settori del diritto interno, dal diritto dell'economia al diritto tributario, dal diritto del lavoro al diritto amministrativo. Un panorama esaustivo è già stato offerto dal primo fascicolo speciale di *Giustiziacivile.com* interamente dedicato all'emergenza Covid-19; sul piano comparatistico si moltiplicano ogni giorno i siti (v. ad es. https://comparativecovidlaw.com), i canali tematici su piattaforme, nonché i libri bianchi e i *working papers* dedicati ad approfondire in prospettiva transnazionale le implicazioni giuridiche dell'epidemia (tra questi ultimi basti citare, anche per l'autorevolezza degli autori, A. VON BOGDANDY-P. VILLAREAL, *International Law on Pandemic Response: A First Stocktaking in Light of the Coronavirus Crisis,* in *Max Planck Institut for Comparative Public Law Res. Paper*, 7, 2020, *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3561650##).*

Una componente importante di questo nuovo diritto dell'emergenza, la quale merita una particolare attenzione, è costituita dalla disciplina "semplificata", o a seconda dei punti di vita 'd'eccezione', della tutela dei dati personali. Questa, composta da tasselli normativi promananti da fonti diverse e operanti su diversi registri (sovranazionale, nazionale, regionale), è essenzialmente preordinata a rendere più capillare ed efficace la sorveglianza epidemiologica, più agevole lo scambio di informazioni tra le autorità sanitarie, più rapido e meno oneroso il processo di sperimentazione clinica di nuovi medicinali e dispositivi medici, in ultimo più fluido ed effettivo l'intero sistema di gestione della crisi sanitaria in atto. Ovviamente quanto maggiore è la compressione del livello ordinario delle garanzie, sia pure per inoppugnabili fini di interesse pubblico, tanto più alto è il rischio che il diritto alla protezione dei dati personali – pilastro centrale del sistema contemporaneo dei diritti fondamentali – soffra delle limitazioni eccessive e non facilmente revocabili (anche sul piano cognitivo e culturale, che non è certo il meno rilevante, perché meno effimero rispetto al periodo di vigenza di una norma) una volta terminata l'emergenza. Operare un bilanciamento tra gli interessi, tutti

legittimi, in gioco è pertanto operazione non semplice e che sta impegnando, a diversi livelli, chi ha compiti di responsabilità pubblica in pressoché tutti gli ordinamenti giuridici (per il quadro offerto dal diritto internazionale v. S. Negri, *Communicable disease control*, in G.L. BURCI-B. TOEBES, a cura di, *Research Handbook on Global Health Law*, Cheltenham, 2018, 265). Non a caso, diversi documenti approvati nell'ambito del Consiglio d'Europa e dell'Unione Europea provano a fissare alcuni punti fermi alla luce dei quali orientare tale bilanciamento in maniera coerente con le esigenze di una società democratica e ispirata al rispetto della dignità della persona e dei diritti umani (si v. rispettivamente COE, Information Documents SG/Inf(2020)11, *Respecting democracy, rule of law and human rights in the framework of the COVID-19 sanitary crisis. A toolkit for member states*, 07/04/20; COE Committee on Bioethics, *DH-BIO Statement on human rights considerations relevant to the COVID-19 pandemic*, 14-4-2020; e EU Commission, *Recommendation on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data*, 8-4-2020, C (2020)2296 final,); EU Commission, *Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection*, 17-4-2020, 2020/C 124 I/01).

Queste pagine si propongono una finalità prevalentemente descrittiva, e soltanto secondariamente adotteranno una prospettiva prescrittiva. L'obiettivo primario è quindi quello di illustrare le principali novità normative, ponendo ordine in una legislazione per forza di cose frammentaria, per poi provare a delineare le opzioni di politica legislativa attualmente al centro dell'agenda governativa e parlamentare. Si premetteranno quindi alcuni cenni sul sistema delle fonti in un quadro di emergenza pubblica; si descriveranno poi gli interventi più direttamente incidenti sul bilanciamento tra protezione dei dati personali e tutela della salute; si accennerà alla discussione in atto circa l'adozione di strumenti *data-driven* volti al contenimento del contagio.

2. La protezione dei dati nel diritto dell'emergenza.

Con la dichiarazione dello stato di emergenza, deliberata dal Consiglio dei Ministri il 31 gennaio 2020 ai sensi dell'art. 7, comma 1, lett. c), d.lgs. n. 1 del 2018 per la durata di 6 mesi, il processo di produzione normativa ha subito un'improvvisa accelerazione e un significativo spostamento del suo baricentro dalla naturale sede parlamentare a quella

governativa. In particolare, a seguito della delibera del CdM hanno acquisito assoluta centralità sul piano operativo le ordinanze di protezione civile, atteso che ai sensi del provvedimento citato per gli interventi funzionali alla gestione dell'emergenza può provvedersi con ordinanze emanate dal Capo del Dipartimento della protezione civile "in deroga a ogni disposizione vigente e nel rispetto dei principi generali dell'ordinamento giuridico", nonché i decreti legge, strumento fisiologicamente deputato dalla costituzione alla normazione in condizioni di urgenza. Nel loro operare sinergico queste due fonti hanno disegnato l'architettura fondamentale del diritto dell'emergenza, che si connota per la sua eccezionalità e la portata derogatoria rispetto a principi e istituti consolidati del nostro ordinamento giuridico. Nel momento in cui si scrive si annoverano, tra i principali provvedimenti varati, 21 atti governativi, 24 ordinanze di protezione civile, 18 direttive del Ministero della Salute e altrettanti provvedimenti dei dicasteri economici (un elenco in costante aggiornamento può trovarsi in *https://www.gazzettaufficiale.it/dettaglioArea/12*).

All'indomani della dichiarazione dello stato di emergenza, il Dipartimento della protezione civile ha adottato varie ordinanze atte a limitare il godimento di diritti e libertà fondamentali con la finalità di contenimento dell'epidemia e contrasto dei rischi per la sicurezza e la salute dei cittadini. Alcune di esse toccano il sistema della protezione dei dati personali. Tra queste merita una menzione particolare l'ordinanza 3 febbraio 2020, che – con il previo parere favorevole del Garante della protezione dei dati personali n. 15 del 2 febbraio 2020 – ha stabilito all'art. 5 che "allo scopo di assicurare la più efficace gestione dei flussi e dell'interscambio di dati personali", i soggetti operanti nell'ambito del Servizio nazionale di protezione civile e delle strutture operative ad esso connesse, possono realizzare, nel rispetto dei principi stabiliti dall'art. 5 del Regolamento (UE) 2016/679, trattamenti di dati personali anche appartenenti alle categorie particolari di cui all'art. 9 del Regolamento e financo dati giudiziari (art. 10) necessari per l'espletamento della funzione di protezione civile nel contesto dell'emergenza. Tali dati potranno essere condivisi tra i soggetti appena menzionati, nonché comunicati a soggetti pubblici e privati nel caso in cui ciò risulti indispensabile, ai fini del contenimento dell'epidemia. Per esigenze di celerità il conferimento di incarichi di trattamento ai sensi dell'art. 2-*quaterdecies* del Codice in materia di protezione dei dati potrà avvenire "con modalità semplificate, ed anche oralmente". Tale disposizione, nel precostituire un'autonoma base giuridica per il trattamento

legittimo dei dati particolari e nel prevedere modalità affievolite di tutela, illustra bene come, nel diritto dell'emergenza, fonti normative secondarie siano state abilitate a apportare limitazioni anche profonde a libertà fondamentali in nome del supremo interesse della tutela della salute e ovviamente nei limiti della proporzionalità.

Per ricondurre tali limitazioni a un quadro più coerente con i principi generali e per reinvestire le Camere della propria naturale potestà deliberativa in sede di conversione del decreto, l'art. 14 d.l. 9 marzo 2020, n. 14 (ora rifuso nell'art. 17-*bis* del disegno di legge di conversione del d.l. n. 18 del 2020, A.C. 2463), ha riformulato tale disposizione, elevandone la fonte e rimarcandone il carattere temporaneo, ossia destinata ad avere una vigenza non superiore alla durata dello stato di emergenza. Si è dunque ribadito che:

a) i dati personali, comuni e "particolari", possono essere trattati e avere una circolazione interna agli organi deputati al contrasto dell'emergenza, tra i quali rientrano oltre ai soggetti precedentemente indicati, anche «gli uffici del Ministero della salute e dell'Istituto Superiore di Sanità, le strutture pubbliche e private che operano nell'ambito del Servizio sanitario nazionale e i soggetti deputati a monitorare e a garantire l'esecuzione delle misure disposte ai sensi dell'articolo 3 deldecreto-legge23 febbraio2020, n. 6»;

b) i medesimi dati possono essere comunicati ad altri soggetti pubblici (si pensi in particolare agli enti territoriali o alle autorità di pubblica sicurezza) e privati (si pensi ai datori di lavoro), nonché diffusi (purché non si tratti dei dati particolari di cui all'art. 9 e 10 Reg.), qualora ciò risulti indispensabile al fine dello svolgimento delle attività connesse alla gestione dell'emergenza in atto;

c) al trattamento si applicano i principi di cui all'art. 5 Reg. (liceità, correttezza, trasparenza, finalità, minimizzazione, etc.);

d) il conferimento di incarichi di trattamento ai sensi dell'art. 2-*quaterdecies* del Codice in materia di protezione dei dati potrà avvenire con modalità semplificate, ed anche oralmente;

e) nel quadro delle attività di cui sopra, le autorità sanitarie e gli altri soggetti autorizzati, qualora trattino dati raccolti presso l'interessato medesimo, possono omettere o rendere in forma semplificata l'informativa prescritta dall'art. 13 GDPR.

Inoltre, per ricostruire il rapporto tra il sistema della sorveglianza epidemiologica e la disciplina della tutela dei dati, è opportuno fare cenno ad almeno due altre ordinanze.

La prima, del Ministero della Salute, del 21 febbraio 2020, concernente la sorveglianza attiva dei soggetti a rischio contagio. L'art. 3, nel ribadire che i dati personali raccolti nell'ambito delle attività di sorveglianza di cui all'art. 1 (quarantena con sorveglianza attiva per soggetti che abbiano avuto contatti stretti con casi confermati di infezione) vengono trattati dall'Autorità sanitaria competente per motivi di interesse pubblico nel settore della sanità pubblica (lett. *i* dell'art. 9, § 2, GDPR), stabilisce che «il termine di conservazione di tali dati è di 60 giorni dalla raccolta, a documentazione acquisita viene distrutta trascorsi sessanta giorni dalla raccolta, ove non si sia verificato alcun caso sospetto».

La seconda, del Dipartimento di protezione civile del 27 febbraio 2020, ha attribuito all'Istituto Superiore di Sanità la sorveglianza epidemiologica e quella microbiologica del SARS-CoV-2, disponendo la creazione di una piattaforma informatica nella quale devono confluire i dati raccolti da tutte le Regioni e dalle Province Autonome di Trento e Bolzano, nonché prevedendo che l'Istituto raccolga i campioni biologici positivi di tutte le persone sottoposte a sorveglianza epidemiologica, analizzandoli, confermandone la positività e tenendo una lista aggiornata dei casi confermati e sospetti. L'art. 4 ribadisce che il trattamento in oggetto risponde ai requisiti dell'art. , § 2, GDPR e prescrive la comunicazione dei dati dall'ISS al Ministro della Salute e, in forma aggregata, al Capo Dipartimento Protezione Civile. Inoltre, si prevede che per agevolare la collaborazione scientifica internazionale i dati, preventivamente resi in forma anonima, possano essere condivisi con il database dell'OMS e dello *European Center for Disease Control*. Anche questa ordinanza incide sul sistema della protezione dei dati, allargando la platea dei titolari del trattamento, la tipologia dei dati raccolti, nonché la direzione (in entrata e in uscita) del flusso comunicativo.

Sempre in quest'ottica, i d.P.C.M. del 4 e dell'8 marzo 2020 riformulano ed estendono le misure già adottate con precedenti provvedimenti del Ministero della Salute, stabilendo per i soggetti che abbiano soggiornato in zone a rischio epidemiologico l'obbligo di comunicare tali informazioni all'azienda sanitaria competente per territorio, nonché al medico di medicina generale o al pediatra di libera scelta. Tali dati verranno poi riversati al servizio di sanità pubblica con modalità definite dalle Regioni.

Infine, il secondo pilastro della normativa dell'emergenza incidente sulla tutela della persona è costituito dalla disciplina 'semplificata' delle sperimentazioni di medicinali e dispositivi utili a fronteggiare la crisi Covid-19. A questo riguardo è particolarmente

importante l'art. 17 d.l. 17 marzo 2020, n. 18, che, limitatamente alla durata dell'emergenza, "al fine di migliorare la capacità di coordinamento e di analisi delle evidenze scientifiche disponibili", riconosce all'AIFA la possibilità di accedere a tutti i dati degli studi sperimentali e degli usi compassionevoli dei medicinali per pazienti con Covid-19. Inoltre, esso attribuisce all'Istituto Nazionale per le Malattie Infettive Lazzaro Spallanzani di Roma le funzioni di comitato etico unico nazionale per la valutazione delle sperimentazioni in oggetto. Ai sensi del quinto comma, infine, si prevede che, «"in deroga alle vigenti procedure in materia di acquisizione dei dati ai fini della sperimentazione", l'AIFA, sentito il Comitato etico nazionale di cui al comma 3, pubblica entro 10 giorni dall'entrata in vigore del presente decreto una circolare che indica le procedure semplificate per la menzionata acquisizione dati nonché per le modalità di adesione agli studi». In data 7 aprile 2020 l'AIFA ha emanato la suddetta circolare, rinviando peraltro ai principi espressi nelle Linee Guida dell'EMA e della Commissione UE sulla gestione delle sperimentazioni cliniche durante la pandemia Covid-19, del 27 marzo 2020, pubblicate in *https://ec.europa.eu/health/sites/health/files/files/eudralex/vol-10/guidanceclinicaltrials_covid19_en.pdf*. Deve notarsi che in tali Linee Guida, all'art. 8, si prevedono deroghe importanti alla disciplina del consenso informato, tanto quanto alla forma (che si ammette orale alla presenza di un testimone) e al momento della sua espressione (successiva nel caso di situazioni di pericolo di vita).

3. Quale bilanciamento tra interessi confliggenti?

È legittimo interrogarsi circa la legittimità sostanziale di tali prescrizioni, e segnatamente dell'art. 14 d.l. n. 14 del 2020 (ora rifuso, come si diceva, nell'art. 17-*bis* del disegno di legge di conversione del d.l. n. 18 del 2020, A.C. 2463). È evidente, infatti, che nel prevedere requisiti di informativa semplificati o nel delineare una circolazione legittima ad ampio spettro dei dati anagrafici e sanitari, essi apportano profonde limitazioni al diritto alla protezione dei dati personali, riconosciuto dall'art. 8 della Carta dei Diritti Fondamentali UE e a livello di maggior dettaglio dal Regolamento (UE) 2016/679. L'art. 23 del Regolamento 2017/679prevede che il diritto dell'Unione o dello Stato Membro limiti, mediante misure legislative – e il ricorso allo strumento del decreto legge elimina i dubbi che si sarebbero potuti avanzare circa

l'adeguatezza delle ordinanze a integrare il requisito di legge -, la portata degli obblighi e dei diritti di cui agli artt. da 12 a 22, nonché dell'art. 5, «qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica per salvaguardare (…) importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato Membro, in particolare un rilevante interesse di (…) sanità pubblica e sicurezza sociale». Che si tratti di interventi 'interinali' finalizzati a soddisfare un rilevante interesse pubblico, e segnatamente di sanità pubblica, è di immediata evidenza ed è opportuno ricordare che il Considerando 46 del Regolamento 2016/679 prevede espressamente che, tra i trattamenti legittimi per motivi di interesse pubblico e per la tutela degli interessi vitali dell'interessato rientrano in particolare quelli «a fini umanitari, tra l'altro per tenere *sotto controllo l'evoluzione di epidemie*e la loro diffusione» (cors. agg.). Ad un livello più generale mette conto notare che le misure adottate con l'art. 14 d.l. 14 convergono – ad es., sotto il profilo del *data sharing* – con le raccomandazioni dell'Organizzazione mondiale della Sanità (*Guidance for Managing Ethical Issues in Infectious Diseases Outbreaks,* 2016, principles n. 5 e 10). Ad un livello più specifico è utile richiamare lo *Statement* dell'European Data Protection Board del 19 marzo 2020, secondo cui le misure adottate dai governi per aumentare la rapidità e l'efficacia delle strategie di contrasto all'epidemia devono ritenersi in linea di principio legittime, in quanto preordinate alla tutela di un interesse pubblico rilevante, a condizione che rispettino i due canoni aurei della proporzionalità e della temporaneità (siano cioè limitate alla persistenza della situazione di emergenza). Inoltre, l'EDPB pone opportunamente in luce come le esigenze di contrasto all'epidemia e tutela della salute pubblica rilevino di per sé quali possibili basi giuridiche del trattamento alternative al consenso dell'interessato, tanto in relazione ai dati comuni (artt. 6, punto 1, lett. *d*, *e*), quanto ai dati particolari. Dispone, infatti, l'art. 9, punto 2, che il divieto di trattamento dei dati particolari non opera qualora il trattamento sia necessario per tutelare l'interesse vitale dell'interessato o di un'altra persona fisica (lett. *c*), per motivi di interesse pubblico (lett. *g*), diagnosi, terapia e assistenza sanitaria (lett. *h*), interesse pubblico nel settore della sanità pubblica (lett. *i*), tutto ciò nel rispetto di parametri quali la proporzionalità e il rispetto del contenuto essenziale del diritto alla protezione dei dati, o la presenza di misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato.

Siamo quindi in presenza di una pluralità di norme che integrano e in parte modificano

il sistema della protezione dei dati, al fine di bilanciare il rispetto dell'autodeterminazione informativa con le esigenze impellenti di tutela della salute pubblica in una situazione di emergenza sanitaria. I principi stabiliti dal Regolamento 2016/679 agli artt. 6, 9 e 23 possono di per sé legittimare non soltanto il trattamento dei dati relativi a persone infette, ma anche le attività di ricerca della catena di contagio intraprese a vari livelli dal medico di famiglia, dalle strutture ospedaliere, o dalle altre strutture sanitarie coinvolte. Le ordinanze e i decreti citati descrivono poi un quadro giuridico flessibile per quanto concerne lo scambio di informazioni tra i soggetti interessati alla sorveglianza epidemiologica e in genere al contrasto attivo alla diffusione dell'epidemia. Altro problema è invece quello di capire cosa sia possibile e opportuno fare per rendere più celere e efficace la ricostruzione della catena dei contatti e l'allerta dei soggetti a rischio, tema su cui ci si intratterrà nel prossimo paragrafo.

4. Le strategie data-driven di contenimento dell'epidemia.

Come in ogni altra ipotesi di gestione di rischio epidemico (si v. WHO, *Guidance for Managing Ethical Issues in Infectious Diseases Outbreaks*, 2016; Art. 18 *International Health Regulations*, 2005), è cruciale l'individuazione dei soggetti che abbiano avuto contatti stretti con i casi confermati, affinché possa provvedersi celermente alla loro allerta e all'adozione di tutte le misure preventive, diagnostiche e terapeutiche che l'autorità sanitaria reputi opportune, come prescritto peraltro da molti dei provvedimenti dianzi citati. Il tracciamento 'manuale' tradizionalmente svolto dal personale sanitario attraverso intervista e sistemi analoghi è ovviamente insostituibile, ma soffre di alcuni limiti strutturali, come la difficoltà per la persona infetta di ricordare con precisione l'intero quadro dei contatti pregressi, la presenza di molti contatti accidentali e ignoti nella loro identità allo stesso soggetto interessato, la carenza di personale dedicato nelle situazioni di maggiore crisi epidemica. Da più parti si è quindi invocato il ricorso all'ausilio che oggi possono offrire le moderne tecnologie digitali basate sulla logica dei *big data*, le quali presentano molte potenzialità al fine di ricostruire in maniera rapida e capillare il quadro dei contatti sociali avuti da un caso confermato nel periodo epidemiologicamente rilevante.

L'esperienza dei paesi asiatici, e in particolare della Cina, della Corea del Sud e di Singapore, benché non omogenea al suo interno, è da questo punto di vista particolarmente istruttiva ed è stata approfondita da numerosi studi scientifici. In

particolare, il governo di Singapore ha sviluppato una app, denominata "TraceTogether", finalizzata al tracciamento dei contatti di prossimità per un lasso temporale predeterminato (A. HOLMES, *Singapore is using a high-tech surveillance app to track the coronavirus, keeping schools and businesses open. Here's how it works*, in *Business Insider*, March 24, 2020). La app può essere installata a seguito di scelta volontaria sui telefoni cellulari ed è basata sulla tecnologia Bluetooth; essa rende possibile conservare sul dispositivo individuale dati protetti da crittografia concernenti i contatti stretti avuti dall'utente nel period epidemiologicamente rilevante, dati poi suscettibili di trasferimento in forma anonima in caso di positività accertata alle autorità sanitarie. La base giuridica del trattamento è costituita in questo schema dal consenso dell'interessato; si deve notare peraltro che la parte sostanziale del Data Protection Act di Singapore del 2012 non è applicabile ai soggetti pubblici (art. 4, § 1, lett. *c*). Il suo utilizzo ha permesso di contenere in maniera efficace, per lo meno in una prima fase, la moltiplicazione dei contagi. Ancora più invasivo è stato il ricorso alle tecnologie digitali in Cina (L. FERRETTI-C. WYMANT et al., *Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing,* in *Science,* 10.1126/science.abb6936 (2020) ; H. TIAN et al., *An Investigation of Transmission Control measures during the first 50 days of the Covid-19 epidemic in China***,** in *Science* 10.1126/science.abb6105 (2020), le quali sono state impiegate non soltanto con finalità diagnostiche e preventive, ma anche per scopi di natura repressiva e controllo dei comportamenti individuali, come nel caso del rispetto delle misure di isolamento fiduciario e quarantena. La stessa 'volontarietà' dell'utilizzo sembra ridursi ad una mistificazione, atteso che in diversi regolamenti municipali si è stabilito che l'utilizzo dei mezzi di trasporto o l'accesso ai luoghi pubblici sia subordinato all'esibizione del QR code con colore appropriato (P. MOZUR-R. ZHONG-A. KROLIK, *In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags, New York Times,* 1° marzo 2020). Peraltro, è bene non dimenticare che l'efficacia delle strategie di contrasto messe in campo in Cina per l'emergenza Covid-19 non può essere imputata unicamente alla capillarità della sorveglianza tecnologica, né al carattere fortemente repressivo delle misure adottate per il contenimento, ma deriva in buona parte dalla presenza di un apparato istituzionale affinato a seguito della prima epidemia SARS. Successivamente alla crisi del 2003, sono state adottate diverse normative finalizzate a rendere più coerente e efficace la risposta pubblica alle emergenze epidemiche: la legge generale del

1989 sulla prevenzione e il trattamento delle malattie infettive è stata largamente revisionata prima nel 2004 e poi nel 2013 (L. ZHANG, *Measures to control infectious diseases under Chinese law*, January 29, 2020, in h*ttps://blogs.loc.gov/law/2020/01/falqs-measures-to-control-infectious-diseases-under-chinese-law/*; D. HIPGRAVE, *Communicable disease control in China: from Mao to now*, 1 *J. Global Health* 224 (2011). Assieme alla legge del 2003 sulle risposte all'emergenza e al regolamento dello stesso anno sulle emergenze sanitarie occasionali, la predetta legge ha costituito la cornice giuridica atta a giustificare l'adozione di misure a largo raggio geografico e alta incidenza sociale, come il blocco di intere aree, municipalità o province della nazione cinese.

Anche alla luce di queste esperienze, è chiaro che in termini astratti il contrasto tecnologico all'epidemia risulterà tanto più efficace quanto più ampia e completa sia la base di dati sulla quale può contare, libera l'interconnessione delle banche di dati (pubbliche e privati), interoperabile la piattaforma, immediata la capacità di risposta delle autorità sanitarie al segnale tecnologico. È altrettanto evidente, però, che siffatte condizioni possono essere soddisfatte soltanto in presenza di una capillare diffusione degli *smart devices* in tutta la popolazione, fiducia del pubblico circa limiti e finalità del loro uso, e soprattutto garanzia che non si determini un sistema di sorveglianza di massa, che sacrifichi le libertà care alla democrazia liberale in nome della trasparenza totale e del contrasto efficace all'emergenza epidemica (cfr. considerando 12-19 della Raccomandazione della Commissione UE dell'8 aprile 2020 *on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data*, C (2020)2296 final, 8/04/20). Per questa ragione le scelte attinenti all'adozione di strumenti di controllo *data-driven* sono soggette a una delicata operazione di bilanciamento degli interessi coinvolti, i quali sono sinteticamente rappresentati da un lato dalla protezione dei dati, dalla dignità della persona e dall'integrità del processo democratico e, dall'altro, dalla tutela della vita e della salute.

Attualmente il dibattito sulle misure tecnologiche di ausilio al contenimento dell'epidemia è al centro dell'agenda governativa e parlamentare, non soltanto nel nostro paese (cfr. art. 76 d.l. 17 marzo 2020, n. 18), ma nella quasi totalità degli ordinamenti occidentali interessati dalla pandemia. Lo *European Data Protection Board* ha emanato di recente apposite *guidelines* per il contrasto tecnologico alla pandemia e il

rispetto della protezione dei dati personali (*Guidance 4/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*, 21-4-2020). La Commissione Europea, con la Raccomandazione dell'8 aprile 2020 e il successivo documento del 17 aprile 2020 ha espresso linee guida – non vincolanti – che dovrebbero essere rispettate dagli Stati Membri, anche al fine di assicurarne l'interoperabilità dello strumento, qualora si decida di fare ricorso ad applicazioni tecnologiche per finalità di prevenzione, allerta e tracciamento dei contatti.

Per i limitati fini di questo scritto, ci si limiterà a segnalare le principali opzioni operative attualmente oggetto di valutazione da parte delle istituzioni competenti, enfatizzando in termini generali che l'eventuale accettabilità di tali strumenti deve intendersi sempre strettamente condizionata al perdurare dell'emergenza e all'attualità degli scopi per i quali essi sono stati elaborati(cfr. il citato parere dello European Data Protection Board).

a) *Raccolta dei dati aggregati sui flussi di comunicazione*. L'ipotesi meno invasiva consiste nell'acquisizione da parte delle società di telecomunicazione – e a giudicare dalle notizie di stampa anche dai providers di servizi Internet e social networks – di dati anonimi e resi in forma aggregata, relativi allo spostamento degli utenti al fine di ricostruire trend di mobilità e analizzare l'andamento epidemiologico tramite cartografie. Un sistema di questo tipo è stato messo a punto in Germania, ove si è previsto il trasferimento di dati aggregati al Roland-Koch-Institut (*Anonyme Handydaten an Robert-Koch-Institut weitergegeben, ZD-aktuell*, 2020, 07057) ed è in discussione in Francia e nel Regno Unito (si veda a questo riguardo quanto riportato dagli organi di stampa circa i contatti avuti dal Governo inglese con O2 e altri gestori di servizi di telefonia: M. SWEENEY-A. HERN, *Phone location data could be used to help UK coronavirus effort*, *The Guardian*, 19-3- 2020). Non sembrano frapporsi particolari ostacoli giuridici a tale prassi, per ciò che gli artt. 9 e 15 della Direttiva 2002/58/CE e l'art. 126 del Codice in materia di protezione dei dati consentono l'acquisizione di dati relativi all'ubicazione degli utenti diversi dai dati di traffico se anonimi, o altrimenti previo consenso dell'interessato (così il parere dello European Data Protection Board, che attribuisce particolare rilievo all'anonimato; analoga è la valutazione del Garante federale tedesco, in *https://www.bfdi.bund.de/DE/Datenschutz/Datenschutz-Corona/Allgemeines/FAQ-Mobilfunkdaten-RKI/FAQ-Mobilfunkdaten-RKI-table.html*).

b) *Geolocalizzazione e tracciamento selettivo degli spostamenti di singoli utenti*. Questa ipotesi è stata ad esempio avanzata, assieme a quella relativa ai droni, con finalità repressive, al fine di controllare il rispetto delle misure di quarantena. In Israele, ad esempio, il Primo Ministro ha autorizzato il ricorso da parte delle agenzie per la sicurezza nazionale ai dati in possesso delle compagnie di comunicazione non già in forma aggregata ma individuale (D.M. HALBFINGER-I. KERSHNER-R. BERGMAN, *To Track Coronavirus, Israel Moves to Tap Secret Trove of Cellphone Data*, *New York Times*, 18-3-2020); tuttavia la Corte Suprema, con *interim order* del 19 marzo 2020, ha bloccato l'applicazione di tale disciplina, anche per ragioni di ordine procedurale, stabilendo l'implementazione in via temporanea soltanto delle misure volte ad identificare i contatti delle persone risultate positive all'infezione (*Ben Meir v. Prime Minister*, HCJ 2109/2020; HCJ 2135/2020; HCJ 2141/20). Invocata come tecnica di controllo a carattere repressivo del rispetto degli obblighi di isolamento, essa non può che apparire in tensione con il principio di proporzionalità (e forse anche con il contenuto essenziale del diritto garantito dall'art. 8 Carta dei diritti UE) che regola il diritto della protezione dei dati e dunque difficilmente accettabile, come anche indicato nel par. 10 della Raccomandazione citata della Commissione. D'altronde essa appare anche poco praticabile qualora sia impiegata con finalità di tracciamento dei contatti, in quanto il ricorso ai dati in possesso delle compagnie di telecomunicazione sconta l'insufficiente granularità della localizzazione registrata dalle celle telefoniche in comparazione con tecniche alternative, le quali potrebbero evidenziare la sussistenza di contatti a rischio nel raggio di pochi centimetri.

c) *Tracciamento di prossimità attraverso apposite applicazioni rese operative su telefoni cellulari o dispositivi indossabili*. Questa è evidentemente la soluzione maggiormente funzionale sul piano tecnologico e non a caso ampiamente dibattuta in varie sedi. Una delle iniziative più importanti a questo riguardo è quella del consorzio europeo Pan-European Privacy-Preserving Proximity-Tracing (PEPP-PT), alla quale si ispira la maggior parte delle proposte operative attualmente oggetto di valutazione da parte dei governi e dei parlamenti degli stati membri. L'idea di fondo consiste nel mettere a disposizione dei cittadini un'applicazione che permetta tramite la tecnologia Bluetooth-Low-Energy di registrare e mantenere in forma criptata sul singolo dispositivo traccia anonima dei contatti stretti (al di sotto di una certa distanza spaziale e per un certo lasso temporale) avuti con altri utenti nel periodo epidemiologicamente

rilevante. In caso di accertata positività, registrata dallo stesso utente attraverso apposito codice dopo aver avuto il responso microbiologico, si aprono varie opzioni: *a*) la app potrebbe automaticamente inviare un segnale anonimo di alert ai contatti stretti, i quali verrebbero invitati a rivolgersi al personale sanitario per le opportune valutazioni; *b*) le autorità sanitarie, accedendo direttamente ai dati conservati su una piattaforma centralizzata (auspicabilmente pubblica) e adoperando una chiave di decrittazione in loro possesso, potrebbero identificare i contatti a rischio e contattarli con celerità per assumere le misure conseguenti.

L'alternativa tra un sistema di archiviazione delle informazioni centralizzato ed uno decentralizzato è evidentemente cruciale per definire le caratteristiche operative e le implicazioni giuridiche della specifica architettura tecnologica, ed è su questo punto, non a caso, che si è sviluppato un acceso dibattito pubblico, non soltanto nel nostro paese. La preferenza delle autorità sanitarie di diversi paesi sembra orientarsi verso la soluzione della piattaforma centralizzata, la quale permetterebbe di monitorare in maniera più capillare l'andamento dell'epidemia e gestire in maniera diretta, piuttosto che attraverso informazioni in-app, la fase dei contatti con i soggetti a rischio. Ad essa il Comitato Europeo non ha opposto obiezioni di principio nella Lettera, datata 14 aprile 2020, del Presidente del Comitato alla Commissione Europea sul Progetto di linee guida in materia di app per il contrasto alla pandemia. Diverse organizzazioni attive nel campo della tutela dei diritti civili e lo stesso Parlamento Europeo, con la Risoluzione 17 aprile 2020 sull'azione coordinata dell'UE per lottare contro la pandemia di COVID-19 e le sue conseguenze (n.2020/2616(RSP) hanno invece ribadito l'opportunità "che la memorizzazione dei dati sia completamente decentralizzata" (punto 52), in modo da ridurre i rischi di uso improprio dei dati, e che il codice sorgente sia mantenuto in formato aperto per sollecitare verifiche indipendenti in punto di sicurezza informatica e rispetto dei principi di *data protection*. Di recente, peraltro, le linee guida del Comitato europeo per la protezione dei dati hanno supportato questa soluzione, auspicando la conservazione dei dati esclusivamente sul terminale dell'utente (EDPB, *Guidance 4/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*, 21-4-2020, punto 27).

Per quanto attiene alla *base giuridica del trattamento*, questa potrebbe essere ravvisata, alternativamente, nel consenso dell'interessato ai sensi dell'art. 5 Direttiva 2002/58/CE e degli artt. 6 e 9 GDPR, il quale potrebbe essere reso al momento della installazione

della app sul dispositivo individuale e dovrebbe essere opportunamente differenziato in funzione delle eventuali specifiche finalità del trattamento (in caso di app multifunzione, come *symptoms checking*, *contact tracing*, telemedicina); oppure, come sembrerebbe più coerente qualora la app sia commissionata o messa a disposizione da un soggetto pubblico per finalità di contrasto all'epidemia, nell'interesse pubblico rilevante, in particolare, per fini di tutela della salute *ex* artt. 6, p.1, lett. *d*, *e*, e 9, par. 2, lett. *i* GDPR, oltre che eventualmente art. 15 Direttiva 2002/58/CE. In quest'ultimo senso si è espresso, ad esempio, il Comitato europeo della protezione dei dati, segnalando l'opportunità di fondare il trattamento non già sulla base giuridica del consenso dell'interessato, bensì su quella dell'adempimento di un compito nell'interesse pubblico (EDPB, *Guidance 4/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*, cit., punti 29 e 33). Ovviamente, qualora sia questa la base giuridica prescelta, risulterà indispensabile adottare preventivamente una disciplina legislativa che stabilisca modalità operative, garanzie e limiti di un siffatto trattamento (e la cornice legislativa andrebbe ad avviso di chi scrive comunque assicurata anche nell'ipotesi del consenso quale base giuridica al fine di risolvere le molte questioni aperte in punto di informativa, comunicazione, conservazione e riuso dei dati particolari, nonché eventuali limitazioni dei diritti dell'interessato ex art. 23 GDPR).

Va chiarito in ogni caso che, come sottolineato tanto dal Parlamento, quanto dalla Commissione e dal Comitato prot. dati (v. da ultimo EDPB, *Guidance 4/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*, punto 31), pur nell'ipotesi di una misura di legge che inquadri l'utilizzo della app in una cornice specifica di interesse pubblico, l'installazione e l'utilizzazione della app dovrà assumere un carattere puramente *volontario* e non potranno essere previste conseguenze pregiudizievoli a danno di quei cittadini che non possano o non vogliano dotarsi di un sistema di tracciamento digitale. Una soluzione diversa sembrerebbe porsi inevitabilmente in contrasto con il principio della proporzionalità e del contenuto essenziale del diritto alla protezione dei dati personali di cui all'art. 8 Carta dei diritti UE e all'art. 23 GDPR, oltre che ledere altri diritti costituzionalmente rilevanti e porsi intrinsecamente in contrasto con il principio di uguaglianza ex art. 3 Cost. (atteso che coloro i quali non fossero in possesso di un telefono cellulare o non avessero le abilità digitali necessarie finirebbero per subire, irragionevolmente, un trattamento deteriore).

Infine, dagli orientamenti degli organi europei come sopra indicati si evincono altri punti fermi che non dovrebbero essere valicati da qualsiasi disciplina nazionale. Richiamandoli in maniera succinta, si deve innanzitutto ribadire:

i) il carattere necessariamente anonimo delle informazioni conservate su dispositivi o piattaforme, prevedendosi modalità tecnologiche che limitino in massimo grado il rischio di re-identificazione;

ii) direttamente collegato a tale assunto è l'esclusione del ricorso a qualsiasi forma di geolocalizzazione dell'individuo, atteso che per le finalità di tracciamento di prossimità non è necessaria la raccolta di dati relativi ai movimenti e alla localizzazione geografica dell'interessato;

iii) nell'ipotesi in cui si prevedano app multifunzione, è essenziale garantire la possibilità di esprimere un consenso chiaramente differenziato per ciascuna delle ipotetiche utilizzazioni dei dati (sintomatologia e diagnostica, tracciamento di prossimità, telemedicina, etc.);

iv) i dati non dovranno essere conservati oltre il periodo strettamente necessario per scopi di controllo epidemiologico e contenimento dell'infezione, e dunque da un lato i dati di contatto dovranno essere cancellati dal sistema decorso il termine possibile di incubazione e dall'altro tutti i dati raccolti dovranno essere eliminati terminata l'emergenza sanitaria;

v) deve tenersi fermo il principio fissato dall'art. 22 GDPR con relativa esclusione di decisioni a carattere interamente automatizzato.

5. Conclusioni.

In conclusione, si deve innanzitutto ribadire, come già segnalato dal Presidente dell'Autorità garante nell'audizione informale alle Camere del 8-4-2020, che il diritto alla protezione dei dati non può essere né inteso, né concretamente utilizzato come un ostacolo al contrasto efficace della pandemia. Tutto all'opposto, diversi sondaggi d'opinione evidenziano come una delle ragioni sottese alla scarsa propensione individuale a dotarsi di una app volontaria di tracciamento consiste nel timore di uso improprio dei dati. Ebbene, è soltanto dotandosi di un'architettura giuridica e tecnologica incentrata sul principio del rispetto rigoroso delle regole in materia di tutela dei dati che si può elevare il livello di fiducia nel sistema, rendendolo appunto *trustworthy* (vera parola d'ordine in queste congiunture drammatiche, che richiedono

uno sforzo collettivo e un'alta coscienza individuale). Le regole adottate o in via di adozione nel nostro sistema, come pure negli altri sistemi dell'Europa Occidentale (diverso è il quadro per alcune esperienze dell'est europeo) sembrano muoversi nella giusta direzione. Non giovano, invece, ipotesi emerse sugli organi di stampa nazionale, come quelle relative alle possibili conseguenze negative della mancata installazione dell'applicazione, né a maggior ragione proposte di accesso straordinario ai dati relativi alla localizzazione degli individui quale quello autorizzato in Israele. Un sistema di disciplina altamente garantistico e incentrato sull'alto livello di protezione dei dati personali è da intendersi come un presupposto indispensabile per creare un ambiente di fiducia istituzionale; ma questo è ovviamente soltanto un tassello di una più ampia strategia che deve essere messa in campo dagli organismi pubblici, volta a rappresentare anche sul piano comunicativo l'alto senso sociale di una vera e propria ipotesi di 'donazione' dei dati per scopi solidaristici. Non diversamente da quanto avviene nel campo della donazione di organi e tessuti, dove una disciplina di garanzia è soltanto il primo tassello di una più ampia strategia informativa e di sensibilizzazione sociale, senza la quale è presuntuoso pensare che il diritto possa di per sé conseguire esiti appropriati.

In secondo luogo, come pure rimarcato nelle linee guida del Comitato eur. prot. dati, bisogna guardarsi da ciò che usa definirsi, con espressione inelegante, il "soluzionismo tecnologico". Il ricorso alle tecnologie di contrasto *data-driven* alla pandemia è assolutamente necessario e indispensabile, ed è la stessa Organizzazione mondiale della sanità che lo auspica. Tuttavia, esso non è sufficiente, se non è contornato da una continua ed assidua partecipazione del personale e delle strutture sanitarie, che devono mantenere l'ultima responsabilità nel comunicare, nell'indirizzare e nel rassicurare gli individui in una congiuntura così complicata (sul punto, anche per un opportuno richiamo alla necessaria 'gradualità' e proporzionalità delle misure, v. l'intervista del Presidente dell'Autorità garante per la protezione dei dati personali A. SORO, *Privacy e democrazia ai tempi della pandemia*, in *https://fondazioneleonardo-cdm.com/it/news/privacy-e-democrazia-ai-tempi-della-pandemia-intervista-ad-antonello-soro/*; nonché EDPB, *Guidance 4/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*, punto 36). Il "diritto a un intervento umano" di cui parla la seconda parte dell'art. 22 GDPR deve essere assunto come stella polare di una proficua interazione tra uomo e macchina, finalizzata alla simultanea realizzazione di

due diritti fondamentali, quello alla salute e quello alla dignità della persona. Perché ciò avvenga rimane cruciale il tema dell'adeguato investimento in strutture e personale, dato che le carenze manifestate in questa emergenza (si pensi soltanto al tema della insufficiente dotazione di dispositivi individuali di protezione a beneficio del personale sanitario e in particolare dei medici di famiglia) non dovrebbero ripetersi in circostanze future (si leggano su questo punto le belle pagine di G. Giraud, *Per ripartire dopo l'emergenza Covid-19*, in *https://www.laciviltacattolica.it/quaderno/4075/*).

Infine, è essenziale ribadire che tutte le restrizioni e le limitazioni apportate al diritto alla protezione dei dati personali sono legittime purché strettamente condizionate alla persistenza dello stato di emergenza. Una volta superata tale fase, esse dovranno essere prontamente rimosse, quale tassello essenziale della strategia di uscita dalla crisi. Ciò non toglie, per altro verso, che questa congiuntura possa avere evidenziato falle o limitazioni nell'architettura istituzionale del GDPR e non è escluso – ce lo ha ricordato di recente Christopher Kuner (*Data Crossing Borders*, in *Verfassungsblog.de*, 15 aprile 2020) – che, come è già successo con la crisi dell'11 settembre 2001, la crisi pandemica globale trasformerà aspetti importanti del sistema europeo della protezione dei dati. Tra i diversi aspetti meritevoli di riflessione, e direttamente collegati al legame biunivoco intercorrente tra globalizzazione e pandemie (cfr. INSTITUTE OF MEDICINE, *The Impact of Globalization on Infectious Disease Emergence and Control: Exploring the Consequences and Opportunities: Workshop Summary*, Washington, 2006), emerge con forza l'utilità di ripensare il sistema dei limiti al trasferimento internazionale dei dati per renderlo più preciso e al contempo flessibile di quanto attualmente riesca a fare l'art. 49 GDPR. Abbiamo appreso da questa pandemia che le esigenze di circolazione dei dati per scopi di ricerca scientifica e in particolare epidemiologica sono particolarmente impellenti, specie quando esistono piattaforme digitali che permettono alla comunità globale degli studiosi e dei ricercatori di condividere informazioni e risultanze empiriche essenziali per il progresso della conoscenza e per l'elaborazione di cure. Richiamarsi allo spirito globale che da sempre ha animato le comunità scientifiche, assicurando il progresso umano, è quanto mai utile specie in questo frangente, che assieme a un grande senso di solidarietà ha fatto riemerge, purtroppo, nella sfera politica, le più grette pulsioni localistiche, le quali hanno assunto varie forme, e tra queste anche, in taluni casi, il "sovranismo digitale.

* Il presente lavoro sviluppa e integra il contributo offerto al Rapporto ISS Covid-19 sulla Sorveglianza Territoriale del Gruppo di Lavoro “Bioetica” dell’Istituto Superiore di Sanità e riflette opinioni personali che non impegnano l’Istituzione citata.