MODELLI NORMATIVI DI *CONTACT TRACING* TRA "*RAGIONE*" E "*VOLONTÀ*"*.

di Virgilio D'Antonio e Livia Saporito**

Il due per due quattro non è vita ormai, signori,
ma l'inizio della morte"
F. DOSTOEVSKIJ, *Memorie dal sottosuolo*
[1919 (prima ed. italiana), p. 44)]

1. Introduzione.

La crisi sanitaria causata dalla pandemia che ha attraversato il pianeta ha imposto ai diversi ordinamenti, nazionali e sovranazionali, risposte emergenziali poderose e, sino a pochi mesi precedenti, impensabili, soprattutto nell'impatto che le stesse hanno fatto segnare rispetto a prerogative fondamentali degli individui[1].

Senza che si sia acceso un dibattito pubblico particolarmente vivo, si è assistito, dunque, in specie nella primissima fase di risposta al diffondersi del virus, a fortissime restrizioni di diritti e libertà, da decenni ritenuti angolari nei moderni contesti democratici e, per questo,

* *Sottoposto a referaggio.*

** Virgilio D'Antonio, Professore Ordinario di Diritto privato comparato – Università di Salerno. Livia Saporito, Professoressa Ordinaria di Diritto Privato comparato – Università della Campania "L. Vanvitelli".. * il presente lavoro, pur se concepito unitariamente dai due Autori, deve essere così attribuito nelle sue singole parti: §§ 1 / 3 V. D'Antonio - §§ 5 / 8 L. Saporito - § 4 ad ambedue.

[1] L'emergenza sanitaria provocata dalla pandemia di Covid-19 ha avuto un impatto profondissimo e, per larghi tratti, assolutamente inedito sulle comunità come sui singoli individui, mutandone dinamiche relazionali, scenari politici, prospettive economiche e culturali, con riflessi importanti e conseguenti anche sul contenuto e sulle forme del diritto. Gli interventi, in questo senso, sono stati numerosissimi ed hanno toccato pressoché tutti gli ordinamenti giuridici a livello globale. A tal fine, l'Associazione Italiana di Diritto Comparato, quella di Diritto Pubblico Comparato ed Europeo e la Società Italiana per la Ricerca nel Diritto Comparato hanno attivato il sito *Comparative Covid Law* (https://comparativecovidlaw.wordpress.com/), al fine di offrire una prima mappatura delle molteplici modifiche normative dettate dalla pandemia.

irrinunciabili e pressoché non suscettibili di limitazioni, quantomeno nella narrazione che, di sé, propongono gli ordinamenti occidentali[2].

E così, sotto la scure della normazione dell'emergenza, sull'altare della tutela della salute (pubblica ed individuale) sono progressivamente state sacrificate la liberà di circolazione, la libertà di riunione, la libertà di culto, la libertà d'impresa, secondo quell'espressione sintetica quanto priva di termini definiti – almeno in termini tecnico-giuridici – che è *lockdown*.

Se osservato dalla prospettiva del giurista, l'annichilimento delle libertà fondamentali degli individui, con affermazione netta della prevalenza del diritto alla salute su qualsivoglia differente prerogativa individuale, è stato il tratto caratterizzante della cd. *fase 1* del contrasto alla pandemia, secondo una dinamica dei rapporti pubblico / privato che, seppur con lievi differenze nelle formule declamatorie, in termini operativi ha visto accomunate gran parte delle realtà giuridiche a livello globale[3].

Questa sostanziale omogeneità di soluzioni precettive ha accompagnato anche la transazione, nei differenti ordinamenti, dalla citata *fase 1* – quella cioè delle misure fortemente repressive giustificate dalla necessità di arginare il contagio in atto – alla *fase 2*, caratterizzata invece dall'attenuazione dei contagi e dalla finalità di instaurare un regime di controllo/monitoraggio sul possibile diffondersi del virus.

Il senso del passaggio dalla *fase 1* alla *fase 2*, ove si provi a proporne una rappresentazione con un campo visuale estremamente ampio, che trascenda singolari specificità pure esistenti in singole realtà ordinamentali, è quello della transizione da apparati normativi di repressione (di determinate condotte corrispondenti alle libertà limitate) a dinamiche di governo del fenomeno pandemico basate invece sul controllo (delle medesime condotte prima vietate, poi consentite purché *sub examen*).

Almeno in termini teorici, proprio la necessità di esercitare un costante controllo delle condotte individuali nuovamente esercitabili ha visto, dunque, il progressivo ripristino

[2] Vedi anche V. D'Antonio e G. Giannone Codiglione, *Internet, libertad y soberania sobre los datos*, in L. Picarella e C. Scocozza (a cura di), *Del pueblo soberano al soberano del pueblo. Evolucion del concepto de soberania en la conteporaneidad*, Bogotà, 2019, p. 159 ss.

[3] Vedi A. Vedaschi, *Il Covid-19, l'ultimo stress test per gli ordinamenti democratici: uno sguardo comparato*, in *DPCE online*, v. 43, n. 2, luglio 2020, p. 1453 ss.

delle libertà fondamentali accompagnato dalla imposizione di limitazioni al diritto alla riservatezza[4].

Questo il tema a fondamento della diffusione delle tecnologie informatiche di *contact tracing*, di monitoraggio dei contatti sociali intrattenuti dagli individui[5].

2. Modelli normativi di *contact tracing* tra "*ragione*" e "*volontà*".

I sistemi di allerta e tracciamento, in termini generali, possono svolgere un ruolo importante nel contenimento della diffusione del contagio durante gli scenari di mitigazione delle misure di restrizione ai diritti fondamentali, soprattutto nella misura in cui – sul versante pubblicistico – consentono all'autorità di identificare e tracciare portatori del virus. Allo stesso tempo, in una dinamica individuale, questi sistemi possono rappresentare anche uno strumento decisivo per consentire ai cittadini di praticare un distanziamento sociale efficace e più mirato.

Orbene, sebbene astrattamente realizzabile anche tramite modalità analogiche, sin dall'inizio della crisi Covid-19, in diverse realtà nazionali sono state sviluppate, sia da parte di autorità pubbliche che da soggetti privati, applicazioni *mobile* che, sfruttando l'enorme diffusione a livello globale (e la pervasività nella quotidianità di ciascuno) dei dispositivi *smartphone*, secondo differenti modalità tecniche, hanno la funzione di tracciare la diffusione del virus e bloccare eventuali catene di contagio[6].

In termini generali, queste applicazioni tendono a svolgere tre funzioni: i) informare i cittadini, fornire loro consulenza e agevolare l'organizzazione del *follow-up* medico delle persone sintomatiche, spesso in combinazione con un questionario di autodiagnosi; ii)

[4] Sulla tensione tra eccezionalità e regola, anche in relazione alla produzione normativa, si rinvia a G. Agamben, *Stato di eccezione*, Torino, 2003. Per alcuni aspetti, sembra tornare attuale il monito del giudice Brandeis nell'*Olmstead case* [*Olmstead v. United States*, 277 U.S. 438 (1928), 474], allorché l'autore con Warren del seminale *The right to be let alone* [4 *Harvard L.R.* 193 (Dec. 15, 1890)], all'alba dei primi sviluppi tecnologici, preconizzava la futura tensione che avrebbe contraddistinto il rapporto tra sovranità statale ed esercizio dei diritti individuali: "discovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet".

[5] Cfr. A.M. Campanale, *Flessibile diritto: il diritto alla protezione dei dati personali nella* lockdown exit strategy *europea*, in *DPCE online*, v. 43, n. 2, luglio 2020, p. 2569 ss.

[6] C. Colapietro e A. Iannuzzi, App *di* contact tracing *e trattamento dei dati con algoritmi: la falsa alternativa fra tutela del diritto alla salute e protezione dei dati personali*, in *Dirittifondamentali.it*, n. 2/2020, p. 816 ss.

allertare le persone che si sono trovate in prossimità di una persona infetta per interrompere le catene di infezione ed evitare la recrudescenza delle infezioni nella fase di riapertura; iii) monitorare la quarantena e controllarne il rispetto da parte delle persone infette, eventualmente in combinazione con funzionalità che valutino le loro condizioni di salute durante il periodo di quarantena[7].

Ove, poi, svolgano anche funzioni di diagnosi, prevenzione, monitoraggio, previsione, prognosi, trattamento o attenuazione della malattia, queste *app* possono essere considerate a tutti gli effetti dispositivi medici, con ricadute normative peculiari.

Chiaramente, l'efficacia di queste applicazioni mobili dipende da diversi fattori, fra i quali è sicuramente decisivo il tasso di penetrazione tra gli utenti, ossia la percentuale della popolazione che utilizza un dispositivo mobile e, al suo interno, la percentuale di utenti che hanno scaricato ed utilizzano costantemente l'applicazione. Se rispetto ai modelli normativi a stretta cogenza in ordine all'utilizzo di queste *app* il problema della diffusione diviene per molti aspetti secondario, allorché si discorra di modelli a base volontaristica (come, ad esempio, quello europeo), il tasso di penetrazione dell'*app* finisce per dipendere in maniera decisiva da ulteriori fattori ed, *in primis*, dalla fiducia degli utenti nella tutela dei propri dati tramite misure di sicurezza adeguate e nel relativo utilizzo esclusivamente per allertare le persone che potrebbero essere state esposte al virus[8].

Considerate le funzioni che queste applicazioni per *smartphone* possono svolgere, è di tutta evidenza come il loro utilizzo possa incidere, in maniera più o meno pervasiva, sull'esercizio di tutta una serie di diritti fondamentali, da quello al rispetto della vita privata e familiare a quelli legati alla libertà di circolazione[9].

Ne consegue la necessità, per ogni singola realtà ordinamentale ed in funzione delle peculiarità che la caratterizzano rispetto alla sfera di tutela (formale e sostanziale) assicurata ai diritti fondamentali in gioco, di identificare un *point of balance* tra pubblico e

[7] Cfr. il considerando n. 12 della Raccomandazione (UE) 2020/518 della Commissione, adottata l'8 aprile 2020 (GU L 114 del 14.04.2020, p. 7).

[8] Ciò non toglie che esistono fattori che influiscono sulla efficacia di queste applicazioni a prescindere dal modello normativo in cui ci si muova: si pensi, ad esempio, al tema del *digital divide* (che rispecchia la diffusione tra la popolazione di *smartphone* in grado di supportare l'*app*), alla capacità delle autorità sanitarie di gestire la mole di dati generati dalle applicazioni ed agire di conseguenza, all'integrazione ed alla condivisione dei dati con altri sistemi e applicazioni, nonché all'interoperabilità interregionale e transfrontaliera con altri sistemi.

[9] Cfr. V. Zeno-Zencovich, *I limiti delle discussioni sulle "app" di tracciamento anti- Covid e il futuro della medicina digitale*, in *MediaLaws*, 26 maggio 2020

privato[10]: in particolare, tra esigenze pubblicistiche di sicurezza e controllo nella diffusione dei contagi e anelito privatistico alla più ampia affermazione possibile delle prerogative individuali[11].

Prendendo le mosse da queste coordinate generali, rispetto al tema specifico delle applicazioni di *contact tracing* collegate all'emergenza Covid-19, la differenza di approccio normativo tra modelli di diffusione di queste *app* a base volontaristica (che potremmo definire *deboli* in termini di cogenza) e quelli a fondamento non volontaristico (dunque, *forti*), di là dalla considerazione più ampia dei diritti fondamentali in discussione, parrebbe rispecchiare una diversa considerazione dell'approccio individuale ai rischi per la salute prodotti dalla pandemia in atto.

Per certi versi, pur nella complessità della visione dostoevskiana del tema, nel provare a prendere a prestito la nota differenza tra ragione e volontà[12] che l'autore propone nelle *Memorie dal sottosuolo*[13], potremmo dire che il modello occidentale si basa su una concezione dell'individuo dominato dalla *ragione*, cioè tendente ad agire sempre nell'ottica del perseguimento di vantaggio (che, nel caso che ci occupa, ha una dimensione al contempo collettiva e individuale); al contrario, il modello orientale è caratterizzato da una visione antitetica dell'individuo, dominato dalla *volontà* che può condurre ciascuno a perseguire condotte irrazionali, intese come quelle che conducono ad esiti non qualificabili obiettivamente come vantaggio (sempre nella duplice accezione collettiva e individuale)[14].

---

[10] Cfr. S. Sica e G. Giannone Codiglione, *La libertà fragile. Pubblico e privato al tempo della rete*, Napoli, 2013.

[11] Vedi T. Pitch, *La società della prevenzione*, Roma, 2008; D. Lyon, *Società sorvegliata. Tecnologie di controllo della vita quotidiana*, Milano, 2002. Cfr. N. Bobbio, (voce) *Libertà*, in *Enc. del Novecento*, Roma, 1978 p. 994 ss.

[12] Nell'ambito di una letteratura particolarmente vasta, rispetto al tema specifico del rapporto tra *ragione* e *volontà* si segnalano L. Pareyson, *Il pensiero etico di Dostoevskij*, Torino, 1967; R. Cantoni, *Crisi dell'uomo. Il pensiero di Dostoevskij*, Milano, 1975; V. Šklovskij, *L'energia dell'errore*, trad. it. di M. Di Salvo, Roma, 1984; M. Bachtin, *Dostoevskij. Poetica e stilistica*, trad. it. di G. Garritano, Torino, 2002; C. Olivieri, *Dostoevskij: l'occhio e il segno*, Soveria Mannelli, 2003.

[13] F. Dostoevskij, *Memorie dal sottosuolo*, op. cit., p. 40: "cosa sa la ragione? La ragione sa solo ciò che ha fatto in tempo a sapere (e magari non imparerà nient'altro; e sebbene non sia una consolazione, perché non dirlo?), mentre la natura umana agisce tutta intera, con tutto ciò che ha in sé, consciamente e inconsciamente, e se pur mente, però vive. Io sospetto, signori, che voi mi guardiate con compassione; mi ripetete che un uomo illuminato ed evoluto, insomma, quale sarà l'uomo futuro, non può coscientemente volere qualcosa che non sia vantaggiosa per sé, che questa è matematica. Ma vi ripeto per la centesima volta che c'è solo un caso, solo uno, in cui l'uomo può augurarsi apposta, coscientemente perfino qualcosa di male, di stupido, perfino stupidissimo, e precisamente: per avere il diritto di augurarsi perfino la cosa più stupida e non essere legato all'obbligo di augurarsi solo e unicamente qualcosa di ragionevole".

[14] Si rinvia a A. Santosuosso, *La regola, l'eccezione e la tecnologia*, in *BioLaw Journal*, Special Issue n. 1/2020, p. 609 ss.

Ecco, allora, i due modelli normativi di risposta che divergono nettamente: un individuo dominato dalla *ragione* non necessita di un apparato normativo caratterizzato da forti elementi di obbligatorietà per perseguire l'interesse proprio e quello collettivo al contrasto alla pandemia; di contrappunto, ove il precetto normativo sia rivolto ad un soggetto mosso dalla *volontà*, evidentemente, la possibilità di scelte contrastanti con il perseguimento del vantaggio individuale e collettivo deve essere arginata tramite l'applicazione di dinamiche precettive fortemente cogenti[15].

In effetti, questa dinamica del rapporto tra governanti e governati nella fase emergenziale può essere declinata anche in una prospettiva di matrice fiduciaria, ove evidentemente i modelli normativi fondati su basi di adesione volontaristica alle misure di contenimento del virus si caratterizzano per un maggiore elemento di *fiducia* in coloro che al precetto (debole) sono chiamati a conformarsi. Al contrario, modelli precettivi (forti), basati sulla stretta cogenza delle misure imposte, presuppongono una sostanziale *sfiducia* nella capacità degli individui di operare scelte razionali rispetto alle esigenze di salute pubblica e individuale[16].

3. La dimensione comunitaria dell'individuo dominato dalla "*ragione*".

Ove osservato nella prospettiva del comparatista e secondo la proposta partizione tra modelli *deboli*" e "*forti* di impianto normativo, il sistema comunitario di monitoraggio dei contagi, nella transizione dalla fase di *lockdown* a quella di progressiva riespansione delle

[15] Vedi V. Mayer-Schönberger e K. Cukier, *Big data*, Milano, 2013. Sono oramai anni che si registra un paradigmatico *sclerotizzarsi* della distorsione del rapporto regola/eccezione, anche rispetto alla primazia tra dimensione statale e quella della libertà individuale. Provvedimenti *eccezionali* di compressione dei diritti individuali sono divenuti regola, come oggi – soprattutto oltreoceano – parrebbe oramai regola l'invasione pubblica della sfera privata giustificata da ragioni di *prevenzione*. Sia consentito il rinvio a V. D'Antonio e P. Troisi, *Il delicato equilibrio tra sicurezza pubblica e rispetto della vita privata nel trattamento dei dati PNR a fini di* law enforcement, in *Comp. dir. civ.*, vol. 3/2019, p. 1031 ss.

[16] Il tema dei rapporti fiduciari al tempo della pandemia è affrontato, in chiave sociologica, da S. Belardinelli – G. Gili, *Fidarsi. Cinque forme di fiducia alla prova del Covid-19*, in *Mediascapes Journal*, n. 15/2020, p. 80 ss., ove si identificano quattro livelli di fiducia, che riguardano in parte anche il livello istituzionale e l'apparato normativo: fiducia interpersonale specifica, fiducia interpersonale generalizzata, fiducia istituzionale specifica, fiducia sistemica (confidare). In tema, N. Luhmann, *Vertrauen. Ein Mechanismus der Reduktion sozialer Komplexität*, Stuttgart, 2000 (ed. or. 1968), trad. it. *La fiducia*. Bologna, 2002, nonché A. Seligman, *The Idea of Civil Society*, Princeton, 1992, trad. it. *L'idea di società civile*, Milano, 1993 e, specificamente per il discorso giuridico, R. Dworkin, *Taking Rights Seriously*, Cambridge, 1977, trad. it. *I diritti presi sul serio*, Bologna, 1982.

prerogative individuali, si inquadra indubbiamente quale assetto del primo tipo, calibrato su una rappresentazione degli individui come soggetti mossi essenzialmente dal dato razionale piuttosto che da quello volitivo.

Per comprendere la filosofia di fondo dell'approccio comunitario al tema del tracciamento dei contatti per contrastare la pandemia è necessario prendere le mosse dalle indicazioni contenute nella Raccomandazione (UE) 2020/518 della Commissione, adottata l'8 aprile 2020[17], relativa appunto ad un pacchetto di strumenti comuni dell'Unione per l'uso della tecnologia e dei dati al fine di contrastare la crisi Covid-19 attraverso un approccio comune. Strettamente connesso alla Raccomandazione è il *Common EU Toolbox for Member States*, adottato il 15 aprile 2020 dall'*eHealth Network*[18] ed in linea con le indicazioni fornite dall'*European data protection board*: si tratta di un documento contenente una serie di principi generali, anche di matrice tecnologica, teso a garantire che sviluppo e utilizzo delle applicazioni di *contact tracing* avvenga nel contemperamento tra tutela dei diritti fondamentali dei cittadini e possibilità di controllo dell'epidemia per i governi e le autorità sanitarie pubbliche competenti[19].

In particolare, gli elementi chiave del modello comunitario si riducono essenzialmente a quattro: volontarietà dell'installazione (*voluntary nature*); approvazione da parte dell'autorità sanitaria nazionale (*government approval*); tutela dei dati personali raccolti (*privacy-preserving*) e distruzione dei dati non appena non saranno più necessari al contrasto all'epidemia (*temporary nature*).

Nel definire un *approccio paneuropeo* alle applicazioni mobili per contrastare il Covid-

[17] Occorre segnalare che già con la Decisione n. 1082/2013/UE del Parlamento europeo e del Consiglio, del 22 ottobre 2013, relativa alle gravi minacce per la salute a carattere transfrontaliero e che abroga la decisione n. 2119/98/CE (GU L 293 del 5.11.2013, p. 1). Con quest'ultima Decisione, erano già state stabilite norme specifiche per la sorveglianza epidemiologica, il monitoraggio, l'allarme rapido e la lotta alle gravi minacce per la salute a carattere transfrontaliero. In base all'art. 2, par. 5, di tale decisione, la Commissione, in collegamento con gli Stati membri, assicura il coordinamento e lo scambio delle informazioni tra i meccanismi e le strutture istituiti nel quadro della decisione e i meccanismi e le strutture analoghi istituiti a livello dell'Unione o nel quadro del trattato Euratom. L'organo per il coordinamento degli sforzi nel contesto delle gravi minacce per la salute a carattere transfrontaliero è il Comitato per la sicurezza sanitaria, istituito dall'art. 17 della decisione citata. Al tempo stesso, con l'art. 6, par. 1, venne istituita una rete per la sorveglianza epidemiologica delle malattie trasmissibili utilizzata e coordinata dal Centro europeo per la prevenzione e il controllo delle malattie (ECDC).

[18] L'*eHealth Network* è una rete di autorità nazionali che opera nell'ambito della *digital health and care* al fine di facilitare la cooperazione dei paesi EU che aderiscono alla direttiva 2011/24/EU (che proprio per questo ne ha previsto l'istituzione). Maggiori informazioni sono reperibili al *link* https://ec.europa.eu/health/ehealth/policy/network_en

[19] Il documento è reperibile al *link* https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf

19[20], dunque, in ossequio al più generale principio di minimizzazione dei dati proprio della normativa comunitaria in materia, vengono identificate le linee portanti che le *app*, sviluppate a livello nazionale, dovranno rispettare: innanzitutto, tutela della vita privata e diritto alla protezione dei dati, così da garantire il rispetto dei diritti fondamentali e la prevenzione della stigmatizzazione; favore per l'utilizzo di misure meno intrusive e comunque efficaci, compreso l'uso dei dati di prossimità, ma senza il trattamento dei dati relativi all'ubicazione o agli spostamenti delle persone, nonché l'uso di dati anonimizzati e aggregati laddove possibile[21]; requisiti tecnici riguardanti le tecnologie appropriate (ad esempio, *Bluetooth* a bassa energia) per stabilire la prossimità del dispositivo, la cifratura, la sicurezza dei dati, l'archiviazione dei dati sul dispositivo mobile, il possibile accesso da parte delle autorità sanitarie e la memorizzazione dei dati; requisiti di *cyber security* efficaci per proteggere la disponibilità, l'integrità, l'autenticità e la riservatezza dei dati; scadenza delle misure adottate e cancellazione dei dati personali ottenuti attraverso tali misure al più tardi nel momento in cui la pandemia sarà dichiarata sotto controllo[22]; prescrizioni relative alla trasparenza per le impostazioni sulla privacy in modo da garantire la fiducia nelle applicazioni.

Siffatti principi vengono ulteriormente specificati in sede di *Toolbox*, con particolare riguardo all'uso volontario delle *app*; all'implementazione ed all'approvazione in stretto coordinamento con le autorità di sanità pubblica; alla piena conformità alle normative dell'Unione europea in materia di protezione dei dati e di tutela della vita privata, previa consultazione del Comitato europeo per la protezione dei dati; alla cancellazione dei dati quando non più necessari.

Inoltre, si chiarisce pure che le applicazioni devono essere basate sugli orientamenti epidemiologici convenuti e sulle migliori pratiche in materia di sicurezza informatica e accessibilità; su soluzioni tecnologiche volte a rafforzare la tutela della vita privata, come

[20] Non a caso, nei documenti comunitari, torna spesso il richiamo al principio di interoperabilità delle applicazioni sviluppate in tutta l'Unione europea (*Cross-border interoperability requirements*).

[21] Il caricamento di dati di prossimità dovrà avvenire solo in caso di infezione confermata e con metodi appropriati per allertare le persone che abbiano avuto contatti stretti con la persona infettata, la quale deve comunque rimanere anonima.

[22] Dovranno essere garantiti un riesame periodico del persistere della necessità del trattamento dei dati personali per il contrasto della crisi Covid-19 e le opportune clausole di temporaneità. Si dovranno inoltre prevedere misure al fine di garantire che il trattamento, quando non più strettamente necessario, venga effettivamente soppresso e i dati personali irreversibilmente distrutti (a meno che, sulla base del parere dei comitati etici e delle autorità preposte alla protezione dei dati, il loro valore scientifico, al servizio dell'interesse pubblico, sia superiore all'impatto sui diritti in questione).

la tecnologia di prossimità *Bluetooth*, e a non consentire il tracciamento della posizione delle persone. Centrale risulta, poi, il discorso intorno alla anonimizzazione dei dati: se è vero che le applicazioni possono allertare coloro che si sono trovati in una situazione di rischio di contagio (quindi, che hanno avuto un contatto rilevante con un individuo infetto) affinché si sottopongano al test o comunque si autoisolino, tutto questo processo si realizza senza rivelare l'identità di alcuno dei soggetti tracciati.

Dunque, i capisaldi del modello comunitario di *contact tracing* restano strettamente collegati ai principi cardinali che animano la disciplina della protezione dei dati personali in ambito comunitario, come di recente ridefiniti dal GDPR: in questo senso, le norme in materia di tutela della sfera personale non sono rinnegate, ma anzi riaffermate anche in fase emergenziale[23].

Non a caso, secondo quanto emerge dal *toolbox*, l'impiego di *app* per il tracciamento dei contatti deve avvenire su base rigorosamente volontaria e senza conseguenze negative per chi decida di non scaricare o utilizzare l'applicazione; ancora, in piena coerenza col binomio *informativa/consenso* (in coerenza con quanto previsto dagli artt. 12 e 13 GDPR), le diverse funzionalità dell'*app* (ad esempio, informazioni sull'epidemia, controllo dei sintomi, tracciamento dei contatti e allerta) non devono essere raggruppate, ma essere sviluppate in modo da consentire di prestare il proprio consenso rispetto a ciascuna funzionalità. Ancora, i dati di prossimità (generati dallo scambio di segnali *Bluetooth* a bassa energia fra dispositivi a una distanza epidemiologicamente significativa e durante il periodo a tal fine rilevante) impediscono il tracciamento degli spostamenti individuali ed, in ogni caso, devono essere conservati o esclusivamente sul dispositivo dell'interessato secondo un sistema di *decentralised processing*[24] oppure raccolti in forma anonima tramite

[23] Ne deriva che l'interessato potrà anche esercitare, in qualsiasi momento, i peculiari diritti che garantisce la normativa comunitaria vigente in materia: il diritto di accesso (art. 15 GDPR), il diritto di rettifica (art. 16 GDPR), il diritto all'oblio (art. 17 GDPR), il diritto di limitazione di trattamento (art.18 GDPR), il diritto alla portabilità dei dati (art. 20 GDPR), il diritto di opposizione al trattamento dei dati personali (art. 21 GDPR), il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato (art. 22 GDPR). In tema, sia consentito rinviare a V. D'Antonio - G.M. Riccio - S. Sica (a cura di), *La nuova disciplina europea della privacy*, Bologna, 2016.

[24] A proposito di questo profilo, nel *Toolbox*, a p. 13, si chiarisce che "the proximity data related to contacts generated by the app remains only on the device (mobile phone). The apps generate arbitrary identifiers of the phones that are in contact with the user. These identifiers are stored on the device of the user with no additional personal information or phone numbers". Questo modello è stato adottato in Italia, Belgio, Svizzera e Germania: la peculiarità di questa impostazione, dove tutto il processo si esaurisce all'interno del *device* dell'utente, è data dal fatto che esclusivamente l'interessato è in grado di sapere che gli è arrivata una notifica di allerta. Chiaramente, questo costituisce un vantaggio rispetto a rischi di compromissione dei dati, ma

un *server* gestito direttamente dall'autorità sanitaria pubblica (*Backend server solution*)[25].

La rappresentazione degli elementi caratterizzanti il modello europeo di *contact tracing* indicano, in maniera nitida, come l'impostazione seguita dall'ordinamento comunitario (e da quelli nazionali all'interno dell'UE) sia quella di un sistema di tracciamento *debole*, fondato in via essenziale sulla volontarietà dell'adesione ai meccanismi di controllo ed allerta.

In termini concettuali, questa opzione, finisce per affidare una delle principali misure di contrasto al diffondersi del virus ad una dimensione esclusivamente privatistica, presupponendo che gli individui, comportandosi secondo *ragione*, in maniera spontanea tendano ad assumere la condotta migliore possibile per la loro salute individuale e per quella collettiva.

Difatti, viste le fortissime limitazioni pure imposte ai diritti fondamentali e proprie della prima fase di contrasto al Covid-19, l'opzione per un modello esclusivamente volontaristico allorché, nella transizione alla cd. *fase 2* di contenimento dell'epidemia, si rischia di scalfire il diritto alla riservatezza, parrebbe trovare fondamento non tanto in una scelta sostanziale di affermazione di centralità del diritto individuale sulla dimensione collettiva di tutela della salute, quanto nella considerazione di fondo della razionalità intrinseca delle condotte individuali, indipendentemente da profili di cogenza normativamente definiti.

Il dato portante, allora, diviene la logica della *accountability*, intesa quale decisa responsabilizzazione individuale, rafforzata dall'ampia autonomia che proprio all'individuo viene garantita nella possibilità di conformare oppure no le proprie condotte a canoni di prudenza che giustificherebbero, tramite l'utilizzazione delle *app* di *contact tracing*, il sacrificio, invero decisamente ridotto, della propria sfera individuale in favore

d'altro canto non consente di avere un quadro centralizzato di raccolta delle informazioni collegate all'epidemia.

[25] Rispetto a questa ipotesi di raccolta dei dati, nel Toolbox si evidenzia che "in this option, the app functions through a backend server held by the public health authorities and on which are stored the arbitrary identifiers. Users cannot be directly identified through these data. Only the arbitrary identifiers generated by the app are stored on the server. The advantage is that the data stored in the server can be anonymised by aggregation and further used by public authorities as a source of important aggregated information on the intensity of contacts in the population, on the effectiveness of the app in tracing and alerting contacts and on the aggregated number of people that could potentially develop symptoms" (pp. 13/14). Aderiscono a questo modello di centralizzazione dei dati, ad esempio, le applicazioni *mobile* elaborate nel Regno Unito e in Francia: chiaramente, il principale problema correlato a queste *app* è quello di una più facile associazione – anche incidentale – tra dati raccolti ed identificativi degli interessati, con rischi di compromissione del caposaldo dell'anonimato.

dell'interesse collettivo ad identificare ed arginare in termini tempestivi nuove catene di contagio[26].

Il tema è, invero, evidentemente più complesso e, al di là di valutazioni astratte sulla tendenza degli individui ad adeguarsi spontaneamente a condotte *premianti* anche per la dimensione collettiva, che è assunto quantomai suscettibile di essere posto in dubbio, l'ordinamento comunitario, come più in generale quelli occidentali, allorché sottoposti ad un poderoso *stress test* che è andato a toccare le fondamenta dei loro assetti democratici, si sono dovuti confrontare con la necessità impellente di ripristinare quanto prima quel sistema di diritti che li giustifica nel loro esistere e li caratterizza in termini di stato di diritto.

4. Dal modello "paneuropeo" alle esperienze orientali.

Nel transitare dal modello comunitario alle esperienze orientali, si registrano soluzioni differenti rispetto al problema del tracciamento dei contagi e dell'utilizzo di tecnologie di *contact tracing*: in termini individuali, il dato caratterizzante è quello di una sostanziale svalutazione del profilo volontaristico per affidarsi a dinamiche normative a forte cogenza. In questo senso, sebbene ci si muova in contesti giuridici caratterizzati da una più acerba affermazione del diritto alla vita privata e, più in generale, da una scarsa attenzione riservata al tema della tutela dei dati personali[27], la prospettiva di approccio normativo parrebbe quella di ordinamenti fondati sul presupposto di rivolgersi ad individui mossi – secondo il dualismo dostoevskiano di cui si è detto – non da spinte basate sulla *ragione*, bensì esclusivamente sulla *volontà*. L'assunto è che, in assenza di un forte appartato cogente che *incanali* gli individui verso condotte conformi all'interesse superiore della tutela della salute, i consociati, in via spontanea, potrebbero tendere verso l'irrazionalità di scelte pregiudizievoli per sé stessi e per la collettività.

[26] In tema, G. Resta, *La protezione dei dati personali nel diritto dell'emergenza COVID-19*, in *giustiziacivile.com*, 5 maggio 2020, p. 10 ss.

[27] Sebbene le locuzioni *privacy* e *data protection* siano considerate fungibili, trattasi, a rigore, di nozioni aventi differente portata. Sul punto cfr. J. Kokott e KC. Sobotta, *The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECHR*, in *Int'L Data Priv. L.*, vo. 3/2013, p. 222, («despite substantial overlaps there also important differences, in particular with regard to the scope of both rights and their limitation»).

Ed allora, la risposta dei paesi orientali al contenimento ed alla gestione della pandemia di Covid-19 costituisce, se raffrontata con quella posta in essere dai paesi appartenenti alla cd. "tradizione giuridica occidentale"[28], un nitido esempio di comparazione *per contrasto*, ove in luogo della centralità della autonomia privata si registra quello della coazione (pubblica) ed, al contempo, la preminenza della tutela della vita privata soggiace all'interesse collettivo alla tutela della salute. Naturalmente, l'opzione prescelta non ha la pretesa di esaurire la complessità delle singole realtà ordinamentali e non esclude l'esistenza di zone grigie, intermedie o più sfumate, legate alle peculiarità delle singole esperienze giuridiche. Essa risponde unicamente a finalità di rappresentazione dei tratti fisionomici più salienti dei modelli in questione e si propone di indagarne le cause.

L'uso di applicazioni mobili di tracciamento ci pone al cospetto di un duplice ordine di contrapposizioni: la prima riguarda la volontarietà/obbligatorietà dell'attivazione di sistemi di tracciamento da parte della popolazione; la seconda concerne l'opzione tra anonimizzazione dei dati raccolti e adesione a *social credit systems*. In via generale – l'analisi dei modelli giuridici nelle aree di riferimento evidenzia invero significative variabili – alla volontarietà nell'uso delle *app* si accompagna la criptazione delle informazioni raccolte, là dove le esigenze di *disclosure* sono assenti, o comunque, marginali nei paesi che adottano sistemi di controllo sociale. Sempre in via esemplificativa, al primo modello si ascrivono i sistemi giuridici europeo e nord americano, al secondo, invece, talune (non tutte) realtà asiatiche.

Nei paesi membri dell'Ue, la strada prescelta per appiattire la curva dell'epidemia è passata attraverso il *lockdown* delle attività, se del caso affiancato dall'utilizzo di tecnologie atte a monitorare i cittadini potenzialmente infetti. Facendo seguito alla Raccomandazione dell'8 aprile 2020 della Commissione, la quale poneva l'accento sulla necessità di adottare un approccio coordinato a livello europeo a sostegno della revoca graduale delle misure di confinamento e a tutela della privacy dei cittadini, essi hanno sviluppato un pacchetto di strumenti (*Toolbox of Practical Measures*) per l'uso di applicazioni mobili e per l'utilizzo di dati anonimizzati e aggregati sulla mobilità delle popolazioni.

Come visto, i requisiti essenziali per le applicazioni mobili di tracciamento dei contatti e

[28] Sulla nozione di *Western Legal Tradition* cfr., diffusamente, A. Gambaro e R. Sacco, *Sistemi giuridici comparati*, in R. Sacco (a cura di), *Trattato di diritto comparato*, Torino, 1996, p. 51 ss, che ne individuano le radici ed i caratteri salienti «in un tipo specifico di mentalità storicamente formatosi nell'Europa del XI secolo, il quale attiene al sempiterno problema dei rapporti tra giustizia, diritto, politica, morale e religione».

allerta stabiliti nel *Toolbox* comunitario sono, tra gli altri, la volontarietà ed il pieno rispetto della vita privata e della tutela dei dati personali. Finalità di distanziamento sociale, atte ad interrompere la catena di trasmissione del virus, si accompagnano, dunque, alla necessità di garantire il rispetto – o almeno la non eccessiva compromissione – dei diritti fondamentali della persona. Non sorprende, pertanto, che la portata rafforzata che assume la riservatezza nella *Western Law* – in quanto diritto costituzionalmente protetto e, nel caso degli Usa, *penumbra right*[29] nato nel solco dell'interpretazione estensiva del V emendamento della Costituzione federale – abbia condizionato vistosamente il dibattito sull'utilizzo delle applicazioni, attivabili solo su consenso dell'interessato (cd. sistema *opt out*).

All'approccio paneuropeo – o auspicato tale – fa da contraltare un *modello Oriente*, che, pur nella diversità di epifanie spesso anche molto differenti le une dalle altre, dipendenti dal contesto socio-culturale di ciascuna realtà, privilegia, in linea di principio, misure coercitive e restrittive di controllo basate su applicazioni, piattaforme e sistemi informativi che possono prescindere dalla volontaria adesione delle parti (cd. sistema *opt in*).

È questo il caso di paesi come la Cina e la Corea del Sud, dove le finalità del controllo sulla popolazione, del tracciamento dei contagi e della mappatura del virus sono passate attraverso l'impiego massiccio ed invasivo di strumenti tecnologici, con conseguente compressione della sfera di riservatezza dei singoli. Allo scopo di obbligare i positivi a restare nelle proprie abitazioni e di impedire ai soggetti non positivi di violare le misure interdittive, si è fatto ampio ricorso alla geolocalizzazione tramite applicazioni e all'utilizzo di droni. *App ad hoc* e dati di rete cellulare sono stati, altresì, utilizzati per operare in via automatica il tracciamento degli spostamenti dei positivi onde identificare le persone con cui essi sono entrati in contatto e isolarle a loro volta. I dati raccolti sono stati infine utilizzati per effettuare una mappatura dei positivi utile alla popolazione ed alle istituzioni.

Nell'approccio normativo al ricorso a meccanismi di *contact tracing*, le esperienze orientali paiono invero accomunate dalla convinzione di fondo che la propagazione del virus possa essere ridimensionata attraverso la virtuosa combinazione di questi strumenti, anche per scongiurare *patterns* di comportamento sociale all'insegna della irrazionalità, quali fuga

[29] L'interpretazione estensiva della clausola sul *due process clause* del *Bill of Rights* ha determinano l'emersione dei cc.dd. *penumbra rights*, diritti che sono tutelati dalla Corte Suprema in quanto rientranti nella sfera di azione del giusto processo (in argomento v. V. Varano e V. Barsotti, *La tradizione giuridica occidentale. Testo e materiali per un confronto* civil law common law, Torino, 2014, p. 345).

dalle città, panico, accaparramento di generi alimentari, rivolte nelle carceri *et similia*; da preferirsi ai metodi di tracciamento analogici, praticati in molti paesi occidentali, che fanno leva sulla somministrazione di questionari al contagiato, reputati lenti, costosi e imprecisi (gli Stati Uniti hanno stimato che richiederebbero 300 miliardi di dollari in quel Paese). Alla base di questi interventi v'è un approccio utilitaristico[30] che giustifica le restrizioni alla libertà degli individui in nome di superiori esigenze di salvaguardia della salute pubblica, il quale stride con il comune patrimonio di valori che è a fondamento della *Western Legal Tradition*[31].

Dunque, pur nella difficoltà di ricondurre alla sintesi del modello unitario il caleidoscopio delle esperienze esistenti, non v'è dubbio che il tratto caratterizzante che identifica la prospettiva di molti ordinamenti orientali sia quella dell'approccio *forte* in termini di cogenza e di incidenza sulla sfera individuale; a differenza del modello comunitario, infatti, per un verso, all'individuo viene negato qualsivoglia spazio di autonomia rispetto all'adesione al sistema di *contact tracing* e, per un altro, nel bilanciamento tra interesse pubblico e sfera privata, v'è una decisa opzione in termini di preminenza della prima dimensione a scapito della seconda. Da questo punto di vista, negli ordinamenti orientali, la transizione dalla fase di *lockdown* rigoroso a quella di mitigazione delle restrizioni spesso non è accompagnata da forme di bilanciamento tra tutela della sfera privata e necessità di monitoraggio pubblico, dal momento che il monitoraggio pubblico è già una costante, a prescindere dalla fase emergenziale, e la percezione della necessità di tutela della sfera privata, tanto più ove intesa in termini di diritto, è decisamente poco marcata e percepita al più in via estremamente residuale, sicuramente soggiacente rispetto alla dimensione pubblica ed all'interesse superindividuale.

Questa connotazione di fondo incide e, per larghi tratti, determina la netta differenza di registro normativo rispetto al modello comunitario, accomunando per contrappunto – ove analizzate in un ideale campo lungo – esperienze giuridiche che, in ogni caso, fanno registrare differenze di approccio importanti ove analizzate nelle loro specificità. In altre

[30] A. Hubert e M. Kerkhoff, *Origin of Modern Public Health and Preventive Medicine,* in *Ethical Dilemmas in Health Promotion,* 1987.

[31] Come osserva, muovendo dall'osservatorio dello stato del Tennessee, W.O. Shults, *Cover Story: Tennessee Law in the Time of The Pandemic Disease; Balancing the Needs of Society with Personal Liberites,* in B.J. Tennessee, vol. 14/2020, 56 misure di contenimento obbligatorie quali la quarantena e l'isolamento "can be administered in a way that preserves core American values such as personal liberty and rights provided for in state and federal constitutions".

parole, anche rispetto al peculiare tema della disciplina del *contact tracing*, discorrere di un *modello Oriente* può avere ragion d'essere esclusivamente in una logica di demarcazione profonda rispetto a quanto avviene in Europa e, più in generale, negli ordinamenti della *Western Legal Tradition*, ma il riferimento unificante finisce per perdere molta della propria utilità, in termini epistemologici, allorché analizzato nella sua essenza propria e specifica, ove riemergono tutte le peculiarità di epifanie giuridiche anche estremamente diversificate le une dalle altre. Ciò è particolarmente vero con riferimento all'esperienza della Repubblica popolare cinese, dove, il tema della privacy nei confronti dell'autorità statale deve essere tenuto distinto – come si dirà – dal tema della privacy nei rapporti tra privati[32], facendo registrare, sotto quest'ultimo profilo, significativi passi verso la creazione di un modello originale, più stringente di quello nord americano e maggiormente proteso verso il modello europeo[33].

5. La risposta "anticipata" di Singapore: *TraceTogetherApp* e *Proactive Screening*.

Nell'esperienza di Singapore, città stato di oltre 5 milioni di abitanti dove convivono le culture occidentale, cinese ed indiana, il fattore tempo ha giocato un ruolo nevralgico nella scelta delle strategie da adottare per la gestione del virus. Nella cd. Svizzera di oriente, peraltro strettamente interconnessa con la Cina continentale ed in particolare con Wuhan, epicentro dell'epidemia, l'opzione è stata, sin da subito, a favore di una risposta aggressiva ed anticipata, complice il ricorso ancora vivo delle recenti epidemie dell'Aviaria e di H1N1. Forti dell'esperienza maturata dal *National Centre for Infectious Diseases* (NCID), il controllo dei contagi è qui avvenuto *sul nascere*, al primo segnale di possibile crisi epidemica, attraverso l'utilizzo delle più avanzate tecnologie per mantenere vigili il controllo ed i sistemi di allerta. Basti pensare che, negli aeroporti, gli arrivi da Wuhan sono stati sottoposti a controlli sanitari prima che la trasmissione del virus da uomo a uomo fosse

[32] Sul punto cfr. E. Pernot-Leplay, *China's Approach on Data Privacy Law: A Third Way Between The U.S. and the E.U.*, in *Penn. St. J.L. & Intl. Aff.*, 2020, vol. 49, p. 1 ss. ("country regulates differently privacy from the state and privacy from private actors").

[33] La tensione del diritto cinese verso il modello europeo in material di privacy è illustrato da G. Greenleaf, *The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108*, in *Int'L Data Priv. L.*, vo. 2/2020, p. 68 ss.

confermata il 20 gennaio, e che già dal primo febbraio, Singapore, insieme a Taiwan e Hong Kong, ha implementato in modo proattivo le restrizioni di viaggio sui passeggeri provenienti dalla terraferma. Queste precauzioni, pur avendo comportato un ingente costo - la Cina continentale costituisce il principale partner commerciale e la fonte primaria del turismo - hanno consentito di applicare il controllo coercitivo ad una ristretta cerchia della popolazione. Singapore ha, inoltre, proceduto ad un rigoroso rilevamento dei malati attraverso un imponente tracciamento dei contatti, affiancato da una altrettanto rigorosa quarantena, che si fonda su un sistema misto tendenzialmente decentralizzato, differente da quello API, offerto da Apple-Google. Il Governo di Singapore, aspramente criticato durante l'epidemia SARS per l'adozione di misure fortemente lesive della privacy (obbligo delle persone poste in quarantena di essere costantemente connessi ad una *webcam* e di procedere alla misurazione della temperatura due volte al giorno)[34], ha a più riprese precisato[35] che, in assenza di chips di geolocalizzazione, non è dato considerare la app prescelta (*TraceTogether*) come un dispositivo di tracciamento (*tracking device*), munito di tag elettronico ed atto ad individuare posizione e spostamenti dei singoli, trattandosi piuttosto di uno strumento utile a seguire a ritroso le tracce del contagio (*contact tracing device*)[36], il quale consente l'*uploading* dei dati solo con la partecipazione ed il consenso dell'interessato. *TraceTogether*, che ha preso il via lo scorso 20 marzo, può essere scaricata da chiunque abbia un numero di cellulare di Singapore e sia in possesso di uno *smartphone* abilitato *bluetooth*. Dopo aver prestato il consenso ed aver attivato il *bluetooth*, l'utente dovrà abilitare le notifiche *push* e le autorizzazioni di posizione. L'*app* funziona scambiando segnali *bluetooth* a breve distanza tra telefoni per rilevare altri utenti dell'*app* che si trovino nelle immediate vicinanze. Le informazioni raccolte sono criptate ed archiviate nei dispositivi per 25 giorni, trascorsi i quali esse sono automaticamente cancellate, salvo essere condivise con il Ministero della Salute (MOH) qualora ad un individuo venga diagnosticato il Covid-19, all'esclusivo scopo di consentire ad una ristretta

[34] M. A. Rothstein, in AA.VV., *Quarantine ad Isolation: Lessons Learned from SARS. A Report to the Centres for Disease Control and Prevention*, 2003, p. 89 ss., in http://stacks.cdc.gov/view/cdc/11429.
[35] Cfr. l'intervista rilasciata dal Ministro degli Affari esteri di Singapore Vivian Balakrishnan a Channel New Asia (8 giugno 2020), nella quale egli puntualizza: "it is not a tracking device. It is not en electronic tag as some Internet commentaries have fretted about […] Without a GPS chips, the device cannot track an individual's location and movements".
[36] I verbi *to track* e *to trace*, pur condividendo l'accezione di seguire delle tracce di identificare un percorso, assumono significazioni differenti: il primo (*to track*) comunica l'idea di seguire una pista bel definita in avanti, fino alla fine, con un orientamento verso il futuro; il secondo (*to trace*) comunica invece l'idea di seguire delle tracce a ritroso, per risalire ad una origine, ad una causa, con un orientamento verso il passato.

cerchia di operatori di ricostruire la catena dei contagi. In questa evenienza, la persona contattata dal Ministero è obbligata a collaborare nella mappatura dei propri movimenti ed interazioni, a fornire qualsiasi informazione di cui sia a conoscenza e a produrre documenti utili alla finalità del tracciamento.

Nelle intenzioni della *Government Technology Agency (GovTech)*, che ha sviluppato l'*app* insieme al MOH, *TraceTogether* consente agli utenti di collaborare attivamente nel processo di tracciamento dei contatti. L'assenza di un database centrale testimonia la scelta a favore di una soluzione digitale che sia rispettosa della privacy e che si giustifica esclusivamente per far fronte all'emergenza (l'*app* cesserà di funzionare al termine dell'epidemia). Ovviamente l'efficacia di tale opzione dipende, in larga misura, dalla risposta della popolazione: una adesione nella misura del 75% dovrebbe, secondo le stime, rivelarsi determinante per il successo dell'operazione. Allo stato risulta, tuttavia, che essa sia stata adottata soltanto da una modesta percentuale (circa il 25%) e che, sul piano tecnico, abbia dato prova di cattivo funzionamento con gli *I-phones*, posto che *Apple*, diversamente da iOS, necessita di un database centralizzato. Pertanto, esclusa l'eventualità di rendere obbligatoria l'attivazione di *TraceTogether,* è allo studio una soluzione che prescinde dal possesso di uno *smartphone* e che persegue le medesime finalità di tracciamento attraverso l'utilizzo da parte del cittadino di un qualsiasi strumento portatile.

6. *App* di tracciamento e *Social Credit System*: la Repubblica Popolare Cinese e la Corea del Sud.

La logica *orwelliana* del *Social Credit System* (SCS), da tempo sperimentato nella Repubblica popolare cinese, pervade anche le scelte operate in materia di *contact tracing* (*rectius*, *contact tracking*). Il sistema di valutazione sociale, nato nel 2007 su proposta del Consiglio di stato cinese**,** autore delle *Guiding Opinions Concerning the Construction of a Social Credit System*, è oggetto, dal 2014, del *Planning Outline for the Construction of a Social Credit System (2014-2020)*, il quale individua quattro aree di intervento: onestà negli affari di governo; integrità commerciale; integrità sociale e credibilità giudiziaria. L'SCS[37]

[37] Come rileva G. Kostka, *China's Social Credit Systems and Public Opinion: Explaining High Levels of Approval*, in *New Media and Soc'y*, 2019, p. 1565 ss., diversamente da quanto avviene nelle democrazie

trova giustificazione, sul piano declamatorio, nella velleità di *migliorare* la società cinese attraverso il vaglio di una ingente mole di informazioni di varia natura (pagamenti, comportamenti, spostamenti, sanzioni), atte a valutare, appunto, la reputazione, il credito sociale di persone, aziende e amministrazioni locali. Nelle ottimistiche previsioni del Governo, esso è destinato ad auto alimentarsi grazie alla proattiva collaborazione di cittadini, aziende ed enti, impegnati a migliorare il proprio *rating score*, se del caso segnalando comportamenti non virtuosi altrui. Nei fatti, trattasi di un meccanismo in grado di monitorare persone fisiche e giuridiche attraverso un complesso sistema di controllo, al quale si riconnettono misure premiali e sanzionatorie conseguenti alla valutazione stessa, mercé l'impiego delle più moderne tecnologie. Il *Social Credit System* si avvale di molteplici canali di approvvigionamento dei dati, e non dell'inserimento delle informazioni da parte di funzionari astrattamente corruttibili, organizzati tramite una rete e condivisibili con tutte le autorità coinvolte. Il monitoraggio dei *Big Data*[38] consente di accreditare un punteggio in tempo reale sì che gli uffici competenti, leggendolo, possono stabilire a quali servizi abbia diritto il cittadino o l'azienda sulla base del *credit score* maturato. In particolare, per quel che concerne le persone fisiche, un *rating* positivo, dipendente da attività prestate ad esempio nei servizi sociali o dall'impegno profuso nel volontariato, dà diritto a servizi gratuiti o garantiti (dalle fast lane negli uffici comunali ai servizi di *bike sharing*), mentre un *rating* negativo, imputabile a morosità nel pagamento di debiti o di bollette per le utenze domestiche) fa scattare preclusioni nell'acquisto di titoli di viaggio, nell'accesso a determinati servizi (come il soggiorno in un hotel o la concessione di un prestito) e ad offerte di lavoro; la sottoposizione a più frequenti controlli (in aeroporto)[39].

occidentali, il SCS non è percepito come uno strumento intrusivo della privacy; al contrario esso incontra il gradimento della popolazione cinese, soprattutto di elevato ceto sociale. Il Governo cinese è, tuttavia, consapevole che vi è il rischio di errori, ragion per cui a Shangai si è tenuto un summit per stabilire "how scores can be checked and mistakes rectified" (testualmente Amy Hawkins, *Chinese Citizens Want the Government to Rank Them*, in *Foreign Pol'y*, May 24, 2017), https://foreignpolicy.com/2017/05/24/chinese-citizens-want-the-government-to-rank-them/.

[38] A. Nicita e M. Del Mastro, *Big Data. Come stanno cambiando il mondo*, Bologna, 2019. Sul massiccio utilizzo di Big Data in Cina cfr. X. Lin, *A Dangerous Game: China's Big Data Advantage and How the U.S. Should Respond*, in *University of Illinois Journal of Law, Technology & Policy*, 2020, p. 253 ss.

[39] I criteri di valutazione per le aziende e gli enti locali riguardano, tra gli altri fattori, l'attenzione all'ambiente, la regolarità nei pagamenti, la sensibilità per il sociale e consentono l'attribuzione di uno score che, se positivo, apre la strada ad agevolazioni e finanziamenti; se negativo, invece, a preclusioni nell'accesso a bandi governativi, a maggiori controlli o a difficoltà nell'accesso al credito. Il sistema è stato adottato anche da aziende private, come il gigante dell'e-commerce Alibaba, il quale ha introdotto lo Zhima Credit (o Sesame credit), attraverso il quale si possono ottenere vantaggi presso le società collegate del gruppo, ad esempio esoneri dalla prestazione di garanzie per servizi di noleggio, sconti e addirittura maggiori *contatti* nel sito di incontri di incontri sponsorizzato dalla compagnia (Baihe). Il sistema premia dunque il cliente

Per realizzare questa profilazione di massa, che potenzialmente coinvolge un quinto della popolazione mondiale, il Governo si avvale di una complessa infrastruttura di reti di dati, fondata sulla cooperazione e sulla condivisione delle informazioni tra numerosi attori (dogane, autorità ferroviarie, compagnie aeree, istituti di credito, ecc.).

In questo contesto si innesta *Alipay Health Code*, l'*app* ideata per contrastare il Coronavirus, la quale, utilizzando i Big Data in possesso dell'autorità sanitaria cinese, assegna ad ogni cittadino un colore (verde, giallo o rosso) sulla base degli spostamenti effettuati, del tempo trascorso in luoghi individuati come possibili focolai epidemici o a contatto con potenziali portatori del virus, al fine di stabilire chi deve essere posto in quarantena e chi può circolare liberamente[40]. I *devices* collegati all'*app*, grazie ad un sofisticato sistema che impiega algoritmi ed altre forme di intelligenza artificiale, obbligano gli utenti a fornire nominativo, numero di telefono e codice di identificazione nazionale, dal quale ultimo, attraverso una ricerca *on line*, è possibile acquisire informazioni suppletive – all'occhio dell'osservatore esterno non indispensabili per finalità di prevenzione e contenimento della malattia – relative alla persona contagiata, quali il volto, foto o notizie sui suoi familiari. A ciò si aggiunga che il Governo, già forte di 200 milioni di telecamere installate nel paese, è alla costante ricerca di *partners* del mondo del Tech che lo coadiuvino in questa imponente operazione di mappatura.

Quanto il successo nell'implementazione di sistemi di *contact tracing* sia frutto dell'intima adesione[41] ideologica della popolazione e quanto invece della proverbiale acquiescenza dei cinesi rispetto alle scelte governative dipende, in termini più generali, dal gradimento che incontra il modello del *Social Credit* in questa parte del globo e, sotto diverso profilo, dalla ancora acerba tutela di cui godono i dati personali e la riservatezza. Se, da un lato, l'approccio cinese costituisce un unicum per la sua struttura tentacolare e centralizzata, una sorta di *Big Brother*, è anche vero che trattasi di un fenomeno di proporzioni oramai globali. Si pensi ai sistemi di merito creditizio, particolarmente utilizzati negli USA[42], dove i

fedele e *degno di fiducia*, chiedendo minori garanzie e offrendo altri benefit, ma non prevede – diversamente dal modello di *social credit puro* – sanzioni per i soggetti con un basso *credito*.

[40] In argomento cfr. G. Zunino, *Coronavirus, app e sistemi per tracciare i positivi: come funzionano (nel mondo, in Italia)*, in A*gendadigitale.ue*, 23.04.2020.

[41] I sondaggi riportano un gradimento dell'80% ed alcune municipalità riportano un sensazionale abbattimento nel ritardo dei pagamenti di debiti da quanto è stato implementato il sistema di *Social Credit*. Naturalmente la spontaneità delle risposte e la veridicità di questi dati sollevano legittimi sospetti nell'osservatore esterno.

[42] Denunciano le lacune legislative ed auspicano un intervento del Congresso per sviluppare il sistema di *credit scoring* nel segno della trasparenza, della correttezza e della non discriminazione M. Hurley e J.

cittadini che intendono accedere ad un finanziamento si preoccupano della *responsabilità* dei loro acquisti online e di come questi verranno valutati dall'istituto di credito, o, in Europa, all'accentramento delle informazioni conseguente alla fatturazione elettronica.

Più significativo dal punto di vista sistemologico è il dato che attiene alla portata del diritto alla riservatezza e alla tutela dei dati personali nelle relazioni interprivate; profilo che, come si è detto, va tenuto distinto dal rapporto tra privacy e autorità statali. Evidenti sono gli sforzi di abbandonare la logica settoriale che caratterizza il modello nordamericano di disciplina della materia, a favore di una regolamentazione onnicomprensiva, sull'esempio di quello europeo. Ne è conferma la recente legislazione, civile e penale[43], che, in assenza di una previsione costituzionale *ad hoc*[44], ha conferito maggiore peso e consistenza al diritto alla riservatezza nel panorama domestico. Trattasi tuttavia di interventi in specifiche materie – banca e finanza, sanità, tutela del consumatore, telecomunicazioni ed internet – privi dell'afflato unitario che contraddistingue il modello europeo. Ad oggi, e malgrado il susseguirsi di proposte legislative, la tutela dei personal data è al GB/T 35273-2020 (cd. PI Specification), che modifica e sostituisce la versione del 2017 GB/T 35273-2017 (*Personal Information Security Specification*)[45]. Tale documento, ricalcato sul GDPR europeo, è, come si evince dallo stesso codice GB/T, di applicazione facoltativa ed è indirizzato tendenzialmente alle sole aziende private, definendo le *best practises* cui attenersi in materia di protezione delle informazioni personali, nel rispetto della legge sulla sicurezza informatica (in vigore dal 1 giugno 2017).

Negli auspici, la *PI Specification* dovrebbe attribuire maggior peso alla volontà degli individui ed introdurre restrizioni all'uso della profilazione degli utenti; tuttavia il GB/T non costituisce di fatto un limite all'attività centralizzata di raccolta e di diffusione dei dati

Adebayo, *Credit Scoring in The Era of Big Data*, in *Yale Journal of Law & Technology*, vol. 18/2016, p. 148 ss.

[43] La nozione di privacy è stata, sino al recente passato, del tutto misconosciuta. Essa fa capolino in una serie di leggi che, senza menzionarla espressamente, pongono le basi per il suo riconoscimento: tra queste si annoverano The General Principles of Civil Law of the Republic of China (GPCL), entrati in vigore nel 1987, e modificati nel 2017; The Criminal Law of the People's Republic of China 1979, modificata nel 2009; The Tort Liability Law of the People's Republic of China 2009, the NCP Decision ad opera della Standing Committee of the National People's Congress 2012; The Cyber Security Law (CSL) 2017.

[44] La Costituzione della Repubblica popolare cinese (1982) sancisce, all'art. 38, il diritto alla dignità della persona; all'art. 40, l'inviolabilità della corrispondenza; all'art. 30, l'inviolabilità del domicilio.

[45] La State Administration for Market Regulation (SAMR) e la Standardization Administration of China (SAC) hanno pubblicato congiuntamente la Information Security Technology - Personal Information Security Specification (GB / T 35273-2020) (PI Specification) proposta dal National Information Security Standardization Technical Committee (TC260) il 6 marzo 2020 come modifica e sostituzione della versione di novembre 2017 (GB / T 35273-2017). La specifica PI entrerà in vigore il 1 ottobre 2020.

personali[46], attestandosi sul piano delle "non-binding rules"[47].

In Corea del Sud, paese culturalmente ed ideologicamente affine alla Cina, il paradigma utilizzato nella lotta contro il coronavirus prevede una spinta attività di *geotracking*, abbinata ad una elevata quantità di test ed all'isolamento individuale. Analogamente al caso cinese, l'impiego di nuove tecnologie non costituisce una novità assoluta, rappresentando piuttosto il naturale sviluppo di strategie già sperimentate durante l'epidemia Mers del 2015 e del progetto *smart cities*[48] avviato dal Governo sin dal 2003, il quale, come è noto, è incentrato sulla raccolta di ingenti quantità di informazioni contenute nei *databases* governativi e non.

La diffusione del Covid-19 non ha, pertanto, colto alla sprovvista le istituzioni sudcoreane, le quali, hanno prontamente – e, come si conviene ad un regime autoritario, senza coinvolgimento della società civile –, adottato[49] l'*app Corona100m*, che, previa prestazione del consenso dell'interessato, registra, tramite GPS, una serie di informazioni che saranno condivise, in tempo reale ed in forma anonima, con tutti gli iscritti. Parallelamente, il Ministero dell'interno e della Sicurezza sudcoreano ha avviato il tracciamento delle persone infette utilizzando i dati personali contenuti nei *databases* governativi e nelle telecamere posizionate in luoghi pubblici, nonché quelli conseguenti alla geolocalizzazione ed alle transazioni operate con carte di credito. Tutti i dati relativi a contagi, decessi, guariti

[46] È di tutta evidenza che tale approccio pone delicati problemi di tutela della riservatezza ed espone al rischio di discriminazione gli individui provenienti da Wuhan e quanti siano transitati nella provincia dell'Hubei. Per prevenire il rischio di una violazione dei dati, la *Cyberspace Administration* ha emanato una circolare nella quale, puntualizzando quanto già affermato dalla *National Health Commission*, si afferma che la raccolta dei dati personali deve ispirarsi ai principi della necessità e della minimizzazione e si invitano le società a ciò preposte a d acquisire il consenso degli interessati ove le informazioni debbano essere utilizzate per scopi diversi dalla prevenzione e dalla gestione del Covid, vale a dire per finalità di ricerca, di monitoraggio, di sviluppo di nuovo prodotti o servizi.

[47] E. Pernot-Leplay, *China's Approach on Data Privacy Law: A Third Way Between The U.S. and the E.U.*, in *Penn. St. J.L. & Intl. Aff.*, vol. 49/2020, p. 1 ss.

[48] La definizione di *smart city* è controversa. Come rileva V. Albino, in AA.VV., *Smart Cities: Definitions, Dimensions, Performance, and Initiatives*, in *Journal. Urb. Tech.*, vol. 22/2015, p. 6, la nozione da preferirsi è la seguente: "A city that monitors and integrates conditions of all of its critical infrastructures, including roads, bridges, tunnels, rails, subways, airports seaports, communications, water, power, even major buildings, can better optimize its resources, plan its preventive maintenance activities, and monitor security aspects while maximizing services to its citizens". La raccolta di dati personali è il fondamento sul quale si poggia il progetto delle *smart cities*, con conseguenti problemi relativi al rispetto della privacy: in argomento cfr. J. Wagner Givens e D. Lam, *Smartier Cities or Bigger brother? How the Race for Smart Cities Could Determine The Future of China, Democracy and Privacy*, in *Symposium Urban Intelligence and The Emerging City*, in *Fordham Urban Law Journal*, vol. 47/2020, p. 829; L. Edwards, *Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective*, in *Eur. Data Prot. L. Rev.*, vol. 28/2016.

[49] M. Cardone e M. Cecili, *Osservazioni sulla disciplina in materia di dati personali in tempi di Covid-19. L'Italia e i modelli sudcoreano, israeliano e cinese: opzioni a confronto*, in *Nomos*, n. 1/2020, p. 10 ss.

sono pubblicati su un sito *web*; come pure sono rese note le generalità (nome, indirizzo, luogo di lavoro) e gli spostamenti delle persone positive al virus, anche dando avviso tramite SMS ai cittadini che abbiano frequentato gli stessi luoghi nei quali è transitato un infetto.

Analogamente a quanto rilevato nell'esperienza cinese, il massiccio ricorso alla tecnologia per ragioni sanitarie ed emergenziali determina una intollerabile compressione del diritto alla riservatezza, tanto a dispetto della vigenza di una dettagliata normativa in materia di privacy e della sua valenza di diritto costituzionale. Sotto il primo profilo è evidente la lesione del principio di minimizzazione dei dati richiamato, tra gli altri, dal *Personal Information Protection Act* (PIPA)[50], il quale impone di limitare l'utilizzo dei dati personali al perseguimento di specifiche finalità e per il tempo strettamente necessario allo scopo prefissato. Quanto al secondo aspetto, è opportuno precisare che la Corte Costituzionale sudcoreana, nella decisione nota come *Fingerprint Case*[51], ha riconosciuto ai *data privacy rights* la consistenza di diritti di rango costituzionale ai sensi degli artt. 10 e 17 Cost. e, con riferimento al caso di specie, ha equiparato le impronte digitali a informazioni personali il cui utilizzo rappresenta una restrizione del "right to information self-determination"[52]. Il peso specifico di questa sentenza è tangibile ove si ponga mente alla funzione nomofilattica di fatto dispiegata dall'Alta Corte all'interno di un sistema nel quale – complice anche l'influenza di Portalis e del *Code civil* nel processo di codificazione coreano[53] – l'elaborazione della legge avviene attraverso un duplice canale: la legge ed i giudici[54].

[50] Nel gennaio 2020, l'Assemblea Nazionale coreana ha emendato le tre fondamentali leggi in materia di privacy *Personal Information Protection Act* (PIPA), *Act on the Promotion of Information and Communications Network Utilization and Information Protection* (Network Act) e l'*Act on the Use and Protection of Credit Information* (Credit Information Act), introducendo il principio di minimizzazione dell'impatto dell'attività di monitoraggio ed il concetto di *pseudonymised data*.

[51] Constitutional Court of Korea, 26/5/2005. Il caso concerneva la legittimità costituzionale dell'impiego delle impronte digitali rilevate ai cittadini adulti coreani per ottenere il rilascio delle Resident Registration Cards nell'ambito dell'attività investigativa della polizia. In questa occasione l'Alta corte ha rilevato che, sebbene il diritto alla privacy sui propri dati non sia espressamente contemplato dalla Costituzione, nondimeno – come rilevano a commento della sentenza H. Ko, J. Leitner, E. Kim e J. Jung, *Structure and Enforcement of Data Privacy Law in South Korea*, Brussels privacy hub, Working paper, vol. 2, 7, ottobre 2016, p. 12, "data privacy rights should nonetheless be recognized as fundamental constitutional rights, which are derived from other rights such as the right to private life (Article 17) and the right to dignity and to pursue happiness (Article 10)".

[52] Principio ribadito più di recente dalla Constitutional Court of Korea, nella decisione del 23 dicembre 2015.

[53] In argomento cfr. K. Kim, *Codification in the 21 st Century. A View from Korea*, in *Codification. The 2012 International Congress of Comparative Law*, Taiwan, May 24-26, p. 3 s.

[54] K. Kim, *Les différents techniques de l'élaboration de la loi: le code et les cases*, in *Droits privés en cours de globalization: perspectives coréano-français*, Colloque international du centenaire de la faculté de Droit de la Korea University et du Bicentenaire du Code Civil Français, 12/3/2005.

7. L'esperienza israeliana: tecnologia e stato di diritto nell'orientamento della Corte Suprema.

Un massiccio uso di tecnologie di sorveglianza per contrastare la diffusione dell'epidemia si registra in Israele, sistema giuridico di complessa qualificazione per via della sua anima composita che lo colloca in una zona spuria, a metà tra sistemi di *civil* e di *common law*. Nel paese è stata lanciata un'applicazione denominata *Hamagen* (scudo), che traccia le posizioni degli utenti per verificare eventuali esposizioni. Le informazioni, memorizzate soltanto sullo *smartphone*, vengono confrontate con quelle in possesso del ministero della Salute: se i dati si incrociano, il ministero fornisce indicazioni per la registrazione e l'auto-quarantena.

Sostanzialmente, l'applicazione sfrutta la geolocalizzazione per tracciare i movimenti di una persona iscritta alla piattaforma, che è risultata positiva al coronavirus. Gli utenti vengono avvisati tramite una notifica se sono stati in contatto con un positivo o se hanno frequentato dei luoghi a rischio contagio ed invitati a recarsi presso le autorità sanitarie per un controllo.

Durante la fase acuta dell'epidemia, il Parlamento israeliano (*Knesset*) ha autorizzato lo *Shin Bet*, l'agenzia di intelligence interna, tradizionalmente impegnata nella lotta contro il terrorismo, ad utilizzare il proprio database segreto per arrestare la diffusione del Covid-19[55]. Sebbene la *Knesse*t abbia individuato un arco temporale di un mese, con scadenza 30 aprile, la decisione della Commissione Affari esteri e Difesa non ha chiarito se la possibilità di estrarre informazioni dai dispositivi mobili di soggetti individuati come positivi potesse protrarsi anche dopo la cessazione dell'emergenza sanitaria. Ciò ha sollevato le vibrate proteste di talune associazioni per la tutela dei diritti civili, dell'opinione pubblica e delle stesse istituzioni, preoccupate della tenuta di un diritto fondamentale quale è la privacy all'interno di uno Stato che si proclama democratico[56]. A tal riguardo non è superfluo precisare che il diritto alla riservatezza trova fondamento nelle *Basic Laws* che

[55] Sul punto v. S. Elder, *Coronavirus Crisis Exposis Shin Bet's Secret Database,* in al-monitor. com (1 aprile 2020).

[56] "Israel is jewish and democratic state" (testualmente R. Hirschl, *The 'Constitutional Revolution' and the Emergence of the New Economic Order in Israel*, in *Israel Studies*, n. 1/1997, p. 136).

compongono la costituzione israeliana[57] e nella *Israeli Privacy Protection Law* (1981). Il 23 marzo, dunque con largo anticipo rispetto alla scadenza fissata dal Parlamento, l'Autorità Garante ha emanato delle linee guida sui profili della privacy potenzialmente coinvolti dalla pandemia, sottolineando come l'eccezionalità delle circostanze imponga di operare un costante bilanciamento tra il controllo del virus e le possibili violazioni della riservatezza, di minimizzare l'impatto di eventuali provvedimenti restrittivi della sfera privata che si rendessero necessari per finalità di prevenzione e controllo del virus e, per quel che concerne i dati personali, di utilizzarli esclusivamente per ragioni riconducibili all'emergenza sanitaria[58]. Reiterando un principio già contenuto *nella Section (2) delle Privacy Protection (Information Security) Regulations* (2017), l'*Authority* ha precisato che i soggetti preposti al controllo dei dati devono valutare, al cessare dell'epidemia, la necessità di trattenere per sé i dati e, in caso negativo, di provvedere alla loro cancellazione. Nei fatti, l'instabilità politica – Israele ha da un anno un governo di transizione – e la aggressività del virus hanno, in un primo momento, indotto l'esecutivo a varare una strategia di contenimento dell'epidemia che, scavalcando la *Knesset* e prescindendo dall'autorizzazione dei tribunali, si è contraddistinta per tempestività e per capacità di adattare il *know how* maturato nel contrasto al terrorismo all'emergenza Covid attraverso il controllo dei cellulari e degli strumenti di mobilità elettronica, tra cui carte di credito e di debito**.** A dispetto del consenso riscosso all'esterno – il modello israeliano è da più parti riguardato come esempio da emulare per la sua efficacia –, potere legislativo e potere giudiziario non hanno tardato a replicare all'esecutivo. Una commissione parlamentare di controllo ha interrotto l'uso delle tecniche di monitoraggio, reputando i benefici derivanti dall'uso delle *app* nettamente inferiori al sacrificio richiesto ai cittadini in termini di violazione della privacy, mentre la Corte Suprema si è resa autrice di una importante decisione, resa pubblica il 26 aprile scorso, nella quale, indagando il difficile rapporto tra libertà individuali e sicurezza collettiva, ha solennemente bocciato la strategia del governo.

[57] All'indomani della Dichiarazione di Indipendenza (1948), i contrasti insorti in sede di Assemblea costituente circa la forma da attribuire alla costituzione israeliana sono sfociati nella emanazione della cd. *Harari Resolution* (13 giugno 1950), in virtù della quale la Constituent Assembly ha mutato il proprio nome in Knesset, optando per l'emanazione di una costituzione composta di capitoli isolati, ciascuno dei quali è denominato *basic law* (Divrei Ha-Knesset, vol. 5, p. 1793: "the Constitution shall be composed of individual chapters, in such a manner thet each of them shall constitute a basic law in itself. The individual chapters shall be brought before the Knesset […] and all the chapters together will form the State Constitution").

[58] Cfr. *Israeli Privacy Protection Authority's Guidelines on Privacy Aspects Of the Coronavirus Epidemic* (COVID-19): "a key principle is that the personal data must be used solely for the purpose for which it was collected".

L'intervento dell'Alta Corte, la quale svolge un ruolo di riequilibrio e di contrappeso decisivo all'interno del sistema israeliano – basti pensare al controllo che essa esercita sull'operato dei tribunali rabbinici[59] – è giunto, non a caso, dopo le ripetute sollecitazioni espresse da esponenti della società civile, condannando la raccolta, lo stoccaggio e l'uso dei dati personali per finalità non strettamente connesse all'emergenza e reclamando un intervento legislativo della *Knesset* sulla materia specifica. In un significativo passaggio, il Presidente della Suprema Corte, Ester Hayut, ha affermato che sebbene la lotta per arginare il virus possa implicare, in via eccezionale, l'adozione di misure straordinarie, in deroga all'ordinaria vita democratica, il fattore tempo deve essere inteso come dirimente; pertanto non può avere corso una iniziativa dai caratteri «invasivi» se non vi è chiarezza incontrovertibile sulla sua durata nonché sulla destinazione delle informazioni raccolte[60]. La scelta dello Stato di utilizzare il suo servizio di sicurezza preventiva, normalmente riservato ai sospetti terroristi di Hamas, ai loro parenti e amici, pone, rispetto agli oltre otto milioni di cittadini coinvolti, evidenti problemi di costituzionalità, oltre che di etica. I rilievi formulati dal massimo organo giurisdizionale circa il rapporto tra sicurezza, salute, tecnologia e Stato di diritto sono ampiamente condivisibili, vieppiù se si consideri che l'invito alla moderazione nell'attività di *contact tracing* proviene dall'autorevole istituzione di un paese la cui popolazione convive con *app* che avvisano i cittadini dell'avvenuto invio di missili, razzi o bombe sul territorio israeliano.

8. Conclusioni.

La *policy* che ispira il tema delle *app* per il *tracing* dei contagiati nei paesi occidentali è nel segno della volontarietà, della trasparenza, del rispetto della privacy e dell'anonimizzazione dei dati. Sotto il primo profilo, la necessaria e proattiva collaborazione del singolo, il quale va reso edotto delle conseguenze connesse all'uso dell'applicazione e, in particolare, al possesso di informazione circa il contagio (proprio e

[59] R. Halperin-Kaddari, *Expressions of Legal Pluralism in Israel: The Interaction Between the High Court of Justice and Rabbinical Courts in Family Matters and Beyond*, in *Jewish Family Law in the State of Israel*, 2002, p. 185.

[60] Secondo i giudici vi è un pericolo evidente di una deriva «scivolosa» nell'utilizzo di un'arma «straordinaria», che potrebbe avere anche dei «risvolti dannosi».

altrui), favorisce l'emersione di un sentimento di responsabilità sociale, che ha una ricaduta positiva sull'intera collettività. Naturalmente, è indispensabile che il singolo possa confidare nella trasparenza del servizio e nell'assenza del perseguimento di scopi ulteriori, incompatibili con la finalità di prevenzione sanitaria. Ciò spiega il *favor* per la gestione del servizio di *contact tracing* da parte di uno o più soggetti pubblici attraverso modalità di *open access*. Il perno del sistema *opt in*, come dimostrano le numerose iniziative intraprese dalle istituzioni europee per indirizzare la scelta delle soluzioni tecnologiche utili al tracciamento dei contatti sociali, resta l'individuazione di un ragionevole *balancing* tra le esigenze di tutela della salute pubblica[61] e la salvaguardia del fondamentale diritto alla riservatezza. Le *app* oggi in uso si caratterizzano infatti per il ricorso alle tecnologie meno invasive, ad esempio Bluetooth a bassa energia; per la temporaneità del trattamento, rigorosamente circoscritto alla durata della pandemia (a meno che, sulla base del parere dei comitati etici e delle autorità preposte alla protezione dei dati, il loro valore scientifico, al servizio dell'interesse pubblico, sia superiore all'impatto sui diritti in questione); per l'impiego esclusivo delle informazioni per finalità di contrasto della crisi Covid-19 e per il divieto del loro utilizzo per scopi differenti, ad esempio per l'applicazione di norme di legge o per fini commerciali. Le soluzioni adottate sono nel segno della *compliance* al GDPR, alla direttiva e-Privacy e ai principi in materia di protezione dei dati e denotano con chiarezza l'opzione a favore di una risposta coordinata e condivisa a livello europeo. Per contro il quadro che emerge non è del tutto esente da ombre. Google ed Apple, come si è detto, si sono accordati per fornire esclusivamente le API delle applicazioni di *contact tracing*. Con una metafora potremmo dire che G. ed A. forniscono un campo su cui giocare, ma le squadre e le regole le decidono gli sviluppatori. In tal modo tutte le questioni relative alla privacy sono traslate sulla responsabilità dello sviluppatore e del Paese che adotta questa o quella *app*. Elevato sono, inoltre, i rischi di inefficienza conseguenti ad un basso tasso di adozione e ad una manipolazione malevola. Il maggior clamore suscitato dalla pretesa lesione della privacy induce a non soppesare adeguatamente il dato che G. ed A.

[61] In argomento, sia pure non espressamente riferibile al caso del Covid-19, v. le osservazioni di M.A. Rothstein, *From Sars to Ebola: Legal and Ethical Considerations for Modern Quarantine*, in *Ind. Health L. Rev.*, n. 12/2015, p. 227 ss., ad avviso del quale la quarantena, misura paradigmatica della necessità di bilanciare gli interessi pubblici e privati, deve essere subordinata a rigorosi requisiti di ordine etico ("1. Necessity, effectiveness and scientific rationale; 2. proportionality and least infringemet; 3. Human supportive services; and 4. Public justification") onde evitare illegittime intromissioni nella libertà individuale.

custodiscono nei propri server una considerevole mole di informazioni socio-sanitarie[62] di valore inestimabile, le quali, sebbene criptate, consentono di profilarci dal punto di vista economico e finanziario, vendendo spazi pubblicitari ritagliati non più sul cittadino ma sulla *persona digitalis*[63]. Potrebbero, allora, ipotizzarsi dei correttivi, come una app che tracci soltanto senza fornire nessuna altra informazione, che cancelli periodicamente i contatti (ad esempio ogni 15 giorni), accompagnata da una diagnosi mirata e veloce[64]: se io ricevo il risultato del tampone dopo 3 giorni, il tracciamento diventa inutile posto che in questo arco di tempo potrei aver infettato altre persone a mia insaputa. Quindi *app*, test rapido e rigorosa quarantena a seguire.

Quanto al *modello Oriente* – se di modello compiuto si può discorrere nei limitati termini di cui si è detto –, è di tutta evidenza che la gestione, sanitaria e politica, della crisi determinata dalla pandemia ha rappresentato, e rappresenta tuttora, un banco di prova sul quale misurare i termini del rapporto tra pubblico e privato nelle società dell'informazione e della conoscenza. Il rapporto tra tutela dell'anonimato e, più in generale, della sfera della privacy, e interessi della collettività è, nelle realtà asiatiche, una questione aperta alla quale ciascuna esperienza fornisce la propria risposta. A dimostrazione della minore compattezza dell'*Eastern World* rispetto ai paesi occidentali, la valutazione delle soluzioni adottate dipende dalle singole realtà: se in alcuni paesi, come Cina e Corea del Sud, la palese compromissione del diritto alla riservatezza è giustificata in nome del superiore interesse della collettività alla tutela della salute – interesse che, per inciso, non è detto coincida con quello delle istituzioni che operano in rappresentanza del Paese –; in altri, come Singapore, si sono messe in campo *ab initio* soluzioni più prudenziali, maggiormente rispettose della necessità di operare un *balancing* tra i contrapposti interessi in gioco, o – è questo il caso di Israele – si è assistito ad un ripensamento delle misure adottate. Qui, all'indomani

[62] Questo profilo è indagato da L. Determann, *Healthy Data Protection*, in *Michigan Tech. L. Rev*., vol. 26/2020, p. 229 ss., il quale rimarca che misure restrittive della libertà personali quali il contact tracing e la quarantena possono indurre i datori di lavoro e le compagnie di assicurazione a sfavorire "individuals with pre-existing health conditions in connections with job offers and promotion sas well as coverage and eligibility decisions". Per una differente prospettiva v. B. L. Atwell, *From Public Health to Public Wealth: The Case for Economic Justice*, in *Ky. L. J*., vo. 208/2020, p. 387, la quale ricorda che il Preambolo della Costituzione federale riconosce esplicitamente il valore del *general welfare of the people* e dunque la dimensione (anche) pubblica del bene salute,

[63] H. Matsumi, *Predictions and Privacy: Should There be Rules About Using Personal Data to Forecast the Future*?, in *Cumberland Law Review*, vo. 48/2017-2018, p. 149.

[64] Nella regione Veneto, ad esempio, è sottoposto a tampone chi e individuato da una piattaforma di biosorveglianza, la quale integra in tempo reale i dati che provengono dai laboratori di microbiologia ed i dati delle anagrafi familiari e aziendali.

dell'intervento della sempre attiva Suprema Corte, si è ribadito un principio che deve essere il faro di ogni democrazia: soltanto l'intervento del legislatore può disciplinare una materia incandescente quale è quella dei dati personali e porre limiti all'uso delle nuove tecnologie a detrimento dei diritti fondamentali della persona umana. Non a caso la stessa Repubblica popolare cinese ha intrapreso, di recente, un percorso volto a disciplinare, attraverso leggi settoriali, la materia della privacy nei rapporti tra privati, anche per ovviare alle rigidità della giurisprudenza domestica ed alla mancanza di una interpretazione giudiziale di tipo evolutivo. La definizione puntuale di cosa debba intendersi per dati personali – attraverso una legge onnicomprensiva come nel caso europeo o *step by spep* sull'esempio nord-americano –, la previsione di sanzioni certe ed una giurisprudenza lungimirante, capace, se del caso, di svolgere funzioni vicarie rispetto al legislatore, rappresentano la base sulla quale edificare la protezione della riservatezza e dei personal data.

Abstract: In ragione dell'emergenza legata al Covid-19, nei diversi ordinamenti nazionali, sono state progressivamente imposte numerose limitazioni alle libertà fondamentali degli individui: la libertà personale, quella di circolazione, quella di riunione, quella di culto, quella di iniziativa economica sono soltanto alcune delle principali prerogative individuali fortemente ridimensionate - se non annullate - nella prospettiva del contrasto al diffondersi del contagio e, dunque, nella logica della preminenza del diritto alla salute (individuale e collettiva). Questi interventi limitativi sono stati percepiti come assolutamente necessari e, pertanto, accolti dai destinatari con sostanziale accondiscendenza, senza che sia emerso alcun dibattito - neppure dottrinale - intorno alla possibilità di ricorso a differenti modelli che, alla imposizione iussu principis, preferissero dinamiche volontaristiche di adesione (pure astrattamente ipotizzabili). Ora, in una fase di progressiva (ri)espansione delle prerogative individuali sopracitate, si DPER online n. 2/2020-Issn 2421-0528 Diritto Pubblico Europeo Rassegna online Fascicolo 2/2020 27 apre il dibattito su possibili interventi (parzialmente) limitativi della riservatezza, soprattutto in relazione all'utilizzo di tecnologie di *contact tracing*. Ebbene, rispetto a questa possibilità (che, nell'ordinamento italiano, ruota intorno all'utilizzo della cd. *app* Immuni), le opzioni adottate dai diversi ordinamenti si atteggiano in maniera differente, con opzioni anche antitetiche tra modelli volontaristici/obbligatori di introduzione dei sistemi di tracciamento o, ancora, in ordine alla scelta tra tutela assoluta dell'anonimato dei soggetti tracciati (propria del modello

europeo) ed implementazione di *social credit systems* e meccanismi di geolocalizzazione individuale (tipici di alcune realtà asiatiche). Eppure, limitazioni della privacy, tutto sommato risibili se paragonate a quelle subite nei mesi scorsi da libertà fondamentali cardinali, sono segnate - soprattutto nella tradizione giuridica occidentale - da un forte disvalore politico-sociale, sì da essere accompagnate un profondo dibattito a più livelli, inedito anche per questa stagione emergenziale.

Abstract: Due to the emergency linked to Covid-19, in the various national legal systems, numerous limitations have been progressively imposed on the fundamental freedoms of individuals: personal freedom, freedom of movement, freedom of assembly, that of worship, that of economic initiative are only some of the main individual prerogatives strongly reduced - if not canceled - in the perspective of contrasting the spread of the infection and, therefore, in the logic of the pre-eminence of the right to health (individual and collective)These limiting interventions have been perceived as absolutely necessary and accepted with substantial condescension, without any doctrinal debate concerning the possibility of using different models based upon voluntary dynamics. Now, in a phase of progressive (re)expansion of the individual rights and liberties, the focus is upon contact tracing technologies and their impact on the right to privacy. Antithetical options have inspired Westerns and Eastern legal systems: the former (especially european systems) based on voluntary models of tracking which guarantee the anonymity of the individuals; the latter on the implementation of social credit systems, that make extensive use of compulsory geolocation and other forms of control (such as China, South Korea). Indeed, these privacy restrictions, laughable when compared with to those suffered in recent months by fundamental freedoms, are surrounded - especially in the Western legal tradition - by political and social disvalues and are accompanied by a deep debate at several levels, surprising even during this emergency season.

Parole chiave: Diritto alla riservatezza – tracciamento dei contatti – modelli volontaristici – modelli obbligatori – sistemi di social credit – nuove tecnologie.

Key words: Right to privacy – contact tracing – voluntary and compulsory models – social credit systems – new technologies.