ISSN 2532-8913
Numero 4/2020

La tempesta perfetta
COVID-19, deroghe alla protezione dei dati personali ed esigenze di sorveglianza di massa[1]

di Gabriele Della Morte

1. Avviso ai naviganti

Una premessa di metodo si impone: di fronte al nuovo tutte le competenze sono vecchie. A causa dell'epidemia da COVID-19 inediti quesiti giuridici si irradiano in ogni direzione. Alcuni di essi, tutt'altro che minori, si pongono sul piano delle possibili deroghe in materia di protezione dei dati personali: è su questi che concentrerò le mie riflessioni.

2. Acque agitate

Poco dopo l'ufficializzazione dello stato di pandemia l'opportunità di ricorrere a sistemi di tracciamento al fine di contrastare la diffusione del virus ha presidiato il dibattito mediatico – ne ha discusso la stampa internazionale, quella interna e finanche l'Organizzazione mondiale della sanità. Secondo alcune fonti giornalistiche sarebbero numerosi gli Stati che, in senso lato, vi fanno ricorso e tra questi si riscontra una grande varietà di situazioni che oscilla dalle ipotesi più blande, quali il controllo di assembramenti grazie ai dati aggregati, sino a quelle più incisive, quali la geo-localizzazione e il tracciamento di spostamenti individuali (si tratta del cd. *contact tracing*, potenzialmente incrementabile anche con i dati GPS di *Facebook*, *Google Maps* ecc.).

Tra le forme più incisive il caso più noto è quello di *Alipay Health Code*, una *App* diffusa in Cina. Si tratta di un software che, una volta installato nello *smartphone*, consente una classificazione degli individui sulla base dei dati relativi allo stato di salute, ai contatti avuti in precedenza ecc. Il fine è quello di contrastare l'epidemia attraverso un monitoraggio costante di movimenti e contatti. A ogni controllo occorre esibire il *QR-code* di riferimento generato dalla *App*. Il colore del codice, assegnato da un algoritmo che calcola un coefficiente di rischio, determina diverse conseguenze: il *QR-Code* rosso obbliga a restare al proprio domicilio; quello giallo garantisce mobilità limitata; quello verde consente libertà di movimento. Se non si è provveduto a installare l'applicazione si è ritenuti *ipso facto* (e … *jure*!) *QR-code* rosso.

3. I dati in alto mare

Le questioni che i sistemi di controllo fondati su algoritmi sollevano sul versante dei diritti – dalla privacy alla tutela dei dati personali, passando per la compressione di fondamentali libertà, ad esempio quella di movimento – sono innumerevoli. In un'ottica complessiva gli indubbi benefici di breve termine vanno comparati agli effetti che si potrebbero sedimentare in una prospettiva di più lunga durata.

In un'articolata riflessione ospitata dal *Financial Times*, il filosofo Yuval Noah Harari adotta questa chiave di lettura, insistendo sui rischi del ricorso a tecnologie di sorveglianza di massa. Sino a ieri, toccando il nostro *smartphone* «the government wanted to know what exactly your finger was clicking on», oggi con il

---

* Una prima versione di questo articolo è apparso originariamente nel blog della Società italiana di diritto internazionale del 30 marzo 2020 (consultabile su www.sidiblog.org). Dello stesso A., *on line*, sono consultabili: "Giuridicamente Immuni? Vantaggi e dubbi sull'efficacia dell'app" (in collaborazione con gli studenti della *Law Clinic* di diritto internazionale), in www.cattolicanews del 10 giugno 2020; e "Necessità e proporzionalità in Immuni", in www.medialaws.eu del 11 giugno 2020. Un più maturo e strutturato lavoro, dal titolo "Quanto *Immuni*? Luci, ombre e penombre dell'app selezionata dal Governo italiano", è stato in seguito pubblicato in *Diritti umani e diritto internazionale*, 2020, vol. 14, n. 2, pp. 303-335.

coronavirus «the focus of interest shifts. Now the government wants to know the temperature of your finger and the blood-pressure under its skin». L'analisi di Harari è, peraltro, approssimata solo *per difetto*: in molti casi (come quello cinese riportato *supra*) il controllo non viene esercitato direttamente dai governi, ma da compagnie private che agiscono in collaborazione con i primi. È questa la ragione per la quale alcuni esperti che si sbilanciano a favore di simili tecnologie (Benanti: «per potere continuare a vivere dobbiamo donare qualcosa di immateriale […]: i nostri dati») sollevano il problema di quale sia il soggetto incaricato di tale compito («Non di certo soggetti privati […] L'ideale sarebbe una grande azienda pubblica»). Purtroppo una simile azienda al momento non c'è, a meno che non si intenda gravare di tale peso l'Autorità garante per la protezione dei dati personali (il cui Presidente ha comunque testimoniato una discreta apertura rispetto a simili sistemi di controllo purché corredati da adeguate garanzie). Abbiamo però un importante novero di disposizioni internazionali le quali, in coordinamento con le norme statali, offrono un valido riferimento. Tralasciando le prime, oggetto di altri studi (v., *ex multis*, quelli citati in apertura), concentreremo l'attenzione sui secondi.

4. La bussola di riferimento

Dopo il distanziamento sociale e il confinamento in dimora, il dibattito sulle strategie di contrasto all'epidemia si è indirizzato sulle misure di sorveglianza e *contact tracing*, atteso che, come ha sostenuto il Direttore dell'Organizzazione Mondiale della Sanità nel *media briefing* del 16 marzo 2020: «you cannot fight a fire blindfolded. And we cannot stop this pandemic if we don't know who is infected».

Ma in che modo tali misure impattano sul regime di protezione internazionale dei dati personali? Quante e quali deroghe sono da considerarsi ammissibili? (sia consentito rimandare, per un primo inquadramento, a Della Morte).

Innanzitutto, il quadro normativo internazionale è composito e va dedotto, nell'assenza di un trattato universale, da un insieme di disposizioni settoriali e regionali in combinazione con norme di *soft law*. Tralasciando il discorso su queste ultime – che pure contribuiscono in via ermeneutica alla formazione dei principi che regolano la *governance senza governo* delle reti – è possibile osservare che sono diverse le convenzioni regionali e settoriali di cui l'Italia è parte.

Un esempio settoriale è rappresentato dall'**art. 17 del Patto internazionale sui diritti civili e politici**, dedicato al divieto di interferenze arbitrarie o illegittime nella vita privata. Nel ***General Comment* n. 16** del Comitato dei diritti umani si ricorda, al par. 1, come il divieto debba essere inteso a tutela di ogni intromissione illegale o arbitraria proveniente tanto dal potere pubblico quanto dalle persone fisiche o giuridiche; al par. 3 si precisa che l'aggettivo «unlawful» deve essere interpretato nel senso per cui alcuna interferenza è ammissibile fuori dai casi nei quali essa è autorizzata dalla legge, e nel successivo par. 4 si puntualizza che anche qualora l'interferenza sia autorizzata deve essere conforme alle disposizioni, agli scopi e agli obiettivi del Patto medesimo. Giacché, aggiunge il par. 7, «all persons live in society, the protection of privacy is necessarily relative» e considerato che nel quadro dell'art. 17 non è prevista alcuna eccezione, si applica il regime di deroghe generali sancito dall'art. 4 dello stesso Patto. Ai sensi di quest'ultima disposizione (sulla quale v. Tammone): «In time of public emergency which threatens the life of the nation and the existence of which is officially proclaimed» gli Stati parte possono derogare agli obblighi sanciti «to the extent strictly required by the exigencies of the situation». Tuttavia anche quest'ultima disposizione deve essere interpretata alla luce del *General Comment* menzionato. Il relativo par. 8 specifica che «relevant legislation *must specify in detail the precise circumstances* in which such interferences may be permitted» (*corsivo* aggiunto), aggiungendo che una simile decisione «must be made only by the authority designated under the law», e ancora che «surveillance, whether electronic or otherwise […] should be prohibited». Ma c'è di più: secondo il Comitato non è solo la sorveglianza a dovere essere regolata dalla legge, quanto anche la raccolta e la conservazione di «data banks and other devices, whether by public authorities or private individuals or bodies» (par. 10).

Quanto alle disposizioni aventi portata regionale, un primo gruppo di norme è riscontrabile in seno al Consiglio d'Europa. È il caso dell'**art. 8 della Convenzione europea dei diritti dell'uomo** dedicato al rispetto della vita privata e familiare. L'art. 8, par. 2, diversamente dal Patto, specifica le condizioni al verificarsi delle quali le interferenze delle autorità pubbliche sono da considerarsi ammissibili: che siano previste dalla legge; che siano necessarie nel quadro di una società democratica; che corrispondano agli scopi tutelati, quali la sicurezza nazionale, la protezione della salute ecc. Va da sé che con il corso del tempo l'ambito d'applicazione dell'art. 8 ha registrato una notevole estensione grazie all'opera di interpretazione euristica dei giudici.

Sempre a livello regionale e sempre *ex multis*, merita un breve richiamo la **Convenzione 108** sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale. Il relativo art. 6 è dedicato alla

protezione delle categorie 'speciali' di dati, tra i quali rientrano a pieno titolo quelli relativi alla salute che richiedono una tutela rafforzata.
Un discorso a parte merita **l'Unione europea**, in quanto la protezione dei dati prevista in tale ambito configura un sistema eccezionale e senza precedenti, alla cui formazione hanno contribuito tanto ragioni di ordine economico (i dati dei consumatori europei sono particolarmente attraenti nel mercato globale), quanto di ordine storico-politico (non bisogna dimenticare che l'Unione poggia le propria fondamenta sulle ceneri dell'Olocausto realizzato attraverso discriminazioni fondate su dati personali).
Il sistema di regole in seno all'Unione orbita, oggi, intorno al *corpus iuris* del **Regolamento generale per la protezione dei dati personali (GDPR)**.
Innanzitutto, **l'art. 23**, disciplinando le limitazioni che uno Stato membro può apportare a diversi principi e regole, richiede che essa rispetti «l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica» per salvaguardare [*inter alia*] la sanità pubblica. Dette limitazioni devono essere previste «mediante misure legislative» (par. 1), che contengano indicazioni relative a : *a*) le finalità di trattamento; *b*) le categorie di dati personali; *c*) la portata delle limitazioni introdotte; *d*) le garanzie per prevenire abusi o illeciti; *e*) l'indicazione del titolare del trattamento; *f*) i periodi di conservazione e le garanzie applicabili; *g*) i rischi per i diritti e le libertà degli interessati; e *h*) il diritto degli interessati di essere informati della limitazione, a meno che ciò possa compromettere la finalità medesima (par. 2).
A ciò va aggiunto che le tecniche di sorveglianza in questione **non concernono i semplici «dati personali»** (e cioè, «qualsiasi informazione riguardante una persona fisica identificata o identificabile», *ex* **art. 4 GDPR, n. 1**), ma quella particolare categoria che, ai sensi dell'**art. 4, n. 15**, è rappresentata dai **dati attinenti alla salute** «compresa la prestazione di servizi di assistenza sanitaria». Tali dati, che secondo il **considerando n. 35** ricomprendono «un numero, un simbolo o un elemento specifico attribuito a una persona fisica» (o ancora «qualsiasi informazione, [ad esempio il «rischio di malattie»] indipendentemente dalla fonte») rientrano nel novero dei cd. **dati soggetti a trattamento speciale**.
Questi, ricorda il **considerando n. 51**, sono informazioni «che, per loro natura, sono particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali». Per tale ragione meritano una tutela rafforzata, prontamente specificata all'**art. 9, par. 2**, dove si enunciano le dieci ipotesi in cui non si applica il divieto di trattamento di tali dati speciali. Nel novero di tali eccezioni a noi pare che assumano particolare rilievo la lettera *h*), che fa riferimento ai trattamenti necessari a scopi di «diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei servizi o sistemi sanitari»; e la lettera *i*), che richiama «l'interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici […] ». La disposizione di cui alla lettera *h*) rinvia al **considerando n. 53** ai sensi del quale nel trattamento di dati sensibili per finalità sanitarie, da un lato, «[i]l diritto dell'Unione o degli Stati membri dovrebbe prevedere misure specifiche e appropriate a protezione dei diritti fondamentali e dei dati personali» e, dall'altro, «gli Stati membri dovrebbero rimanere liberi di mantenere o introdurre ulteriori condizioni, fra cui limitazioni, con riguardo al trattamento di dati […] relativi alla salute, senza tuttavia ostacolare la libera circolazione dei dati personali all'interno dell'Unione […]». Diversamente, la disposizione di cui alla lettera *i*) richiama il **considerando n. 54** ai sensi del quale in simili casi il trattamento potrebbe avere luogo «senza il consenso dell'interessato» purché nel rispetto di «misure appropriate e specifiche a tutela dei diritti e delle libertà delle persone fisiche».

Il tema è ripreso in seguito dall'**art. 9, par. 4**, che attribuisce agli Stati membri il potere di introdurre «ulteriori condizioni, comprese limitazioni, con riguardo al trattamento dei dati […] relativi alla salute». Tale ultima disposizione menziona ben cinque considerando (n. 8, n. 10, n. 41, n. 45 e n. 53) dei quali almeno uno merita attenzione. Mi riferisco al **considerando n. 41** che, facendo riferimento ai casi in cui il Regolamento richiama «una base giuridica o a una misura legislativa», specifica che questa non deve essere necessariamente intesa come un «atto legislativo da parte di un parlamento, fatte salve le prescrizioni dell'ordinamento costituzionale», purché risulti «chiara e precisa, e la sua applicazione prevedibile, per le persone che vi sono sottoposte, in conformità della giurisprudenza della Corte di giustizia dell'Unione europea e della Corte europea dei diritti dell'uomo».

Il concetto d'altra parte è ribadito anche dall'**art. 52** della **Carta dei diritti fondamentali dell'Unione europea** – il primo strumento che distingue tra privacy (art. 7) e tutela dei dati personali (art. 8) – laddove si prevede che eventuali «limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà», aggiungendo che dette limitazioni devono essere adottate «nel rispetto del principio di proporzionalità [e] solo laddove siano

necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui».

Da ultimo merita un cenno la **Direttiva *ePrivacy* del 2002,** il cui **art. 15** garantisce agli Stati membri la possibilità di limitare – attraverso il ricorso a «disposizioni legislative» – gli obblighi in materia di riservatezza dei dati sul traffico per finalità determinate e purché in «una misura necessaria, opportuna e proporzionata all'interno di una società democratica». Sebbene il coordinamento tra il GDPR e la Direttiva *ePrivacy* contempli più di una questione aperta, l'opinione dell'***European Data Protection Board*** sul punto è orientata verso il riconoscimento di un valore di *lex specialis* in favore della Direttiva (del Comitato europeo per la protezione dei dati personali v. anche lo *Statement*, alquanto scarno in verità, proprio sulla gestione in tempo di COVID -19).

5. Come segnare il nord

Alla luce delle considerazioni esposte, nel ricorso a un trattamento per così dire 'rafforzato' di dati personali e sanitari occorrerà innanzitutto accertarsi che siano rispettati quanto meno i seguenti requisiti:

(i) **Formalità**: le interferenze devono essere previste da una base giuridica variamente intesa;
(ii) **Indispensabilità**: le interferenze devono essere necessarie nel quadro di una società democratica;
(iii) **Finalità**: le interferenze devono corrispondere allo scopo di protezione della salute;
(iv) **Tassatività**: le interferenze devono essere specificate nel modo più dettagliato;
(v) **Temporalità**: le interferenze devono indicare il periodo di vigenza;
(vi) **Impugnabilità**: le interferenze devono essere contestabili in qualche forma;
(vii) **Proporzionalità**: le interferenze non devono mai essere eccessive rispetto allo scopo perseguito.

Chiaramente alcuni di questi principi possono sovrapporsi o articolarsi in una relazione di *genus* a *species*, oltre a modularsi diversamente a seconda del tipo di interferenza: *contact tracing* più o meno invasivo; trattamento di soli dati personali o anche di dati anonimi e/o pseudo-anonimi; trattamento subordinato al consenso di tutte le persone potenzialmente interessate ecc. Si è comunque deciso di stilare un primo elenco per costituire le basi per una più meditata riflessione successiva (*work in progress*).

6. Quale approdo?

In conclusione c'è certamente qualcosa di contro-intuitivo nel fatto che le democrazie occidentali ricorrano a strumenti propri del *Capitalismo della sorveglianza* (mi riferisco qui al significativo studio di Shoshana Zuboff) per difendere se stesse. Ma questo paradosso è solo apparente, perché frutto di un espediente retorico – piuttosto in voga, purtroppo – che pone la questione nei termini di *trade-off* tra salute e privacy, mentre a un più attento esame appare evidente che la questione non può essere articolata in termini alternativi/oppositivi.
Come salvaguardare *sia* la tutela dei dati personali *sia* la salute, a fronte di una minaccia pandemica? Certamente un approccio ispirato al criterio di gradualità – come quello evocato da Oreste Pollicino e Caterina Resta – fornisce una strategia ragionevole per ogni situazione inedita: occorre innanzitutto testare l'efficacia delle misure meno invasive e quindi incrementarle in caso di bisogno.
Al contempo bisogna contemplare limiti invalicabili perché se è vero che talvolta gli Stati fanno ricorso a legislazioni d'urgenza per ristabilire in un secondo momento un adeguato sistema di garanzie (è accaduto anche in Italia: si consideri la stagione del terrorismo), oggi è il matrimonio tra regolamentazione d'urgenza e innovazione tecnologia che richiede particolare attenzione: dalla prima si può tornare indietro, dall'innovazione tecnologica, *historia magistra*, no.
In definitiva, in attesa che passi la 'tempesta perfetta' si possono anche ammainare le vele. Ma occorre prestare molta attenzione alla bussola per ritrovare, in seguito, la rotta.

(16 dicembre 2020)