Tecnologie di sorveglianza e contenimento della pandemia

di *Carlo Blengino*

Internet e le tecnologie digitali hanno assunto, nel drammatico periodo che stiamo vivendo, un ruolo centrale. Le soluzioni tecnologiche di sorveglianza adottate dagli Stati per contenere la pandemia possono, se non adeguatamente governate e regolamentate, minare e limitare le libertà e i diritti fondamentali riconosciuti alle persone nelle società democratiche. Un'analisi dei limiti tecnologici e normativi di un soluzionismo spesso sopravvalutato.

1. Convivere col virus e con la sorveglianza digitale

Con la prima fase emergenziale della lotta per il contenimento della pandemia, nel periodo del "*lock-down*", abbiamo tutti finalmente compreso come la costante connessione in rete di persone, macchine e oggetti sia ormai parte essenziale ineludibile della nostra vita: non c'è più soluzione di continuità tra la vita *on-line* e la vita *off-line*. Pare essersi improvvisamente (e forzosamente) realizzata negli ultimi mesi la profezia che fece nel 2012 Eric Schmidt, già amministratore delegato e presidente di Google Inc.: «*In futuro* (...) *la tecnologia non avrà soluzione di continuità. Sarà semplicemente già lì. Il Web sarà tutto, e sarà anche nulla. Sarà come l'elettricità e*» proseguiva Schmidt «*se comprenderemo bene questo punto, credo che potremo risolvere tutti i problemi del mondo*»[1].

Risolvere tutti i problemi del mondo con la tecnologia appariva allora – otto anni fa – e ancora può apparire oggi affermazione utopica e velleitaria, ma se osserviamo ciò che ci attende nella prossima fase di convivenza con il virus e analizziamo il proliferare di soluzioni tecnologiche che quotidianamente vengono proposte in relazione all'emergenza sanitaria per monitorare e contenere l'epidemia, quella frase assume una valenza assai più concreta, e per certi versi inquietante.

L'applicazione "Immuni", il sistema di allerta di potenziale contagio basato su dati di prossimità dei nostri *smartphone* realizzato dal Governo sulla base del protocollo predisposto da Apple e Google e di cui molto si discute, è solo una delle tante soluzioni tecnologiche che quotidianamente vengono proposte da Stati, enti privati e aziende per organizzare e monitorare la nostra vita nel prossimo incerto futuro con la pandemia.

1. E. Schmidt, *The World Around Us*, discorso tenuto al convegno «Zeitgeist 2012», 15 ottobre 2012, disponibile *online* all'indirizzo: www.youtube.com/watch?v=kUHF43xjMJM.

Diverse applicazioni simili a "Immuni", legate ai nostri *smartphone* o a dispositivi dedicati (come braccialetti elettronici o semplici "*token*" dotati di sensori) sono state realizzate senza adeguate valutazioni da alcune Regioni come la Sardegna[2] e da diverse aziende private[3] per tracciare spostamenti e contatti di cittadini, utenti e dipendenti; in molti luoghi delle nostre città sono comparsi *scanner* per l'accesso a luoghi pubblici, che rilevano i nostri dati biometrici per monitorare lo stato di salute di avventori e clienti; negli asili, nelle scuole e in alcune fabbriche fanno la loro comparsa telecamere intelligenti in grado di rilevare il distanziamento sociale degli alunni e degli operai[4]; e se a Singapore cani-robot pattugliano i parchi per segnalare assembramenti[5], in Italia i droni vengono autorizzati per controllare persone o zone e quartieri sottoposti a isolamento e quarantena[6]. In generale, *software* evoluti in grado di analizzare e incrociare diverse banche dati sono proposti dalle aziende del settore alle varie autorità sanitarie per tracciare la vita dei cittadini, degli infetti e dei sani, e fornire informazioni (dati) per controllare l'epidemia[7].

Sono tutti sistemi di sorveglianza di massa resi possibili dalle tecnologie digitali e, sebbene molti percepiscano agevolmente – quasi istintivamente – i rischi propri di tali tecnologie sulla nostra vita privata e sulle nostre libertà, cogliendone le implicazioni distopiche di orwelliana memoria, non è semplice, a fronte di una finalità certamente fondamentale e condivisa quale la tutela della salute pubblica, trovare chiari parametri e inequivoci limiti di liceità per tali soluzioni, per ognuna di esse, nel nostro ordinamento.

È necessario infatti individuare correttamente i beni giuridici coinvolti nell'adozione di ogni singola soluzione tecnologica e valutare le concrete implicazioni, non sempre evidenti, della loro implementazione concreta nella vita delle persone. È necessario, insomma, aver contezza di quanto profonda sia la rivoluzione digitale in atto.

Per far ciò occorre conoscere e dominare quella tecnologia, cogliere la potenza e la fragilità che una semplice riga di codice informatico può generare in una banale applicazione per *smartphone* o aver contezza delle distorsioni cognitive che un algoritmo evoluto di *machine learning* che opera su grandi moli di dati può indurre nelle scelte dei decisori o banalmente, con la profilazione e il cd. *micro-targeting*, nell'esercizio quotidiano delle nostre decisioni.

E occorre anche aver chiari i rapporti di forza e di potere tra i diversi attori dell'innovazione tecnologica, tra i governi (più o meno democratici) e le note *Big Tech* che detengono la tecnologia: nell'attuale emergenza sul tema del *contact tracing*, la soluzione tecnologica di due sole società commerciali della Silicon Valley, Google e Apple, ha di fatto dettato e imposto scelte prettamente politiche, di sanità pubblica, ai parlamenti e ai governi del mondo, imponendosi su ogni dibattito democratico.

Lo stato di emergenza, l'eccezionalità che ha caratterizzato la prima fase della pandemia e che ha giustificato significative compressioni di diritti fondamentali da tempo consolidati come la libertà di movimento, sembra inoltre destinato a perdere, in relazione alle attività di controllo e sorveglianza, la sua valenza temporanea, limitata e straordinaria, vuoi per l'incertezza circa i tempi della nostra convivenza col virus nell'attuale pandemia, vuoi per la prospettiva, da più parti ipotizzata, di rischi epidemici divenuti endemici nella nostra società globale e iper-connessa. È reale il rischio che misure temporanee di sorveglianza accettate inizialmente per limitati periodi emergenziali diventino progressivamente prassi e

---

2. L'*app* "Sardegna Sicura" è disponibile sugli *app-store* di Google e Apple. Tra i molti articoli, vds. *Ecco Sardegna Sicura: "traccia" i movimenti nell'Isola*, *L'Unione Sarda*, www.unionesarda.it/articolo/news-sardegna/cagliari/2020/06/12/ecco-la-app-sardegna-sicura-traccia-i-movimenti-nell-isola-136-1028508.html.

3. Sono diverse la aziende private che hanno sviluppato *app* e dispositivi proprietari di controllo. Vds., ad esempio: *Lavorare in sicurezza. L'App anti-Covid di Node "contagia" le cooperative*, *Avvenire*, 16 giugno 2020, www.avvenire.it/economia/pagine/lavorare-in-sicurezza-testa-anti-covid-gratuito.

4. *Sicurezza anticontagio, a Biella la prima scuola italiana "governata" dall'intelligenza artificiale*, *La Repubblica* (Torino), 13 giugno 2020, www.torino.repubblica.it/cronaca/2020/06/13/news/sicurezza_anticontagio_a_biella_la_prima_scuola_governata_dall_intelligenza_artificiale-259115823; e, ancora, negli stabilimenti di Amazon: *Amazon deploys AI 'distance assistants' to notify warehouse workers if they get too close*, *The Verge*, 16 giugno 2020, www.theverge.com/platform/amp/2020/6/16/21292669/social-distancing-amazon-ai-assistant-warehouses-covid-19.

5. *Cane robot fa guardia contro violazioni di distanziamento sociale: la scelta* hi-tech *di Singapore*, *Rai news*, 10 maggio 2020, www.rainews.it/dl/rainews/media/Cane-robot-fa-guardia-contro-violazioni-di-distanziamento-sociale-la-scelta-hi-tech-di-Singapore-016a39a2-02fd-4ffa-862c-b91192a5a886.html.

6. *Cfr.* le linee guida per la ripresa del traffico negli aeroporti a partire dalla "Fase 2" (LG 2020/001-APT), 12 giugno 2020 (ed. n. 4), https://www.enac.gov.it/la-normativa/normativa-enac/linee-guida/lg-2020001-apt.

7. Un acceso dibattito tra gli esperti del settore ha suscitato l'appalto conferito dal Governo britannico alla società Palantir Technologies Inc., una delle società più aggressive e discusse che lavora su *big data* e *machine learning* – *cfr.* www.cnbc.com/2020/06/08/palantir-nhs-covid-19-data.html.

consuetudini delle nostre società, modificando i rapporti interpersonali e, soprattutto, il rapporto bio-politico dei cittadini con l'autorità e lo Stato.

2. Dall'*habeas corpus* all'«*habeas data*»: per non sacrificare il corpo digitale in nome della salute

Se è forse eccessivo attribuire alla rivoluzione digitale un cambio antropologico nell'uomo, è vero che l'impatto delle nuove tecnologie sui singoli e sulla società è assai più profondo e complesso di quanto possa apparire allo sguardo del semplice fruitore e, talvolta, anche a quello di chi propone e realizza, spesso con le migliori intenzioni, nuove efficienti soluzioni digitali[8].

Le nostre interfacce tecnologiche, i cellulari, i *tablet* e in generale gli oggetti connessi da cui siamo circondati estendono i nostri sensi e consentono di superare con un "click" i nostri limiti cognitivi; lo spazio visibile e udibile si amplia oltre ogni limite fisico grazie a schermi e a connessioni sempre più efficienti e pervasive, e le informazioni, i dati costantemente generati dal semplice utilizzo delle tecnologie digitali, sono memorizzati e fruibili grazie all'elaborazione di macchine computazionali sempre più potenti, continuamente alimentate da nuovi dati.

La rivoluzione digitale, con le sue tecnologie dell'informazione, possiede una particolarità: è come se vivessimo immersi in una sorta di magma viscoso ma impercettibile, in grado di rilevare e memorizzare ogni nostra azione, ogni nostro gesto corporeo e fin anche ogni nostra reazione emotiva mediata dai nostri dispositivi. I dati che disseminiamo più o meno scientemente – e, paradossalmente, indipendentemente dall'uso volontario di tali tecnologie, che sono ormai presenti nelle strade per la nostra sicurezza e, oggi, a tutela della nostra salute, negli oggetti di uso comune per renderli "*smart*" e in ogni comunicazione digitale a distanza –, quei dati sono parte della nostra vita, sono frammenti di noi disseminati nel mitico "*Big Data*" e nell'infosfera e possono esser recuperati ed elaborati da macchine e *software* anche a distanza di tempo, per ricostruire un'immagine più o meno completa e un'identità più o meno fedele di noi.

Anche i limiti fisiologici della memoria e i costi/benefici dell'oblio sembrano azzerarsi: fatti o accadimenti per noi oggi insignificanti che riteniamo destinati all'oblio (pensiamo a una banale passeggiata in centro città, ad una occasionale conversazione con un amico o a un semplice acquisto con carta elettronica) possono riemergere nelle immagini captate di una telecamera di sicurezza, nei *file* di *log* di un qualunque servizio della società dell'informazione e, dopo la pandemia, nei sensori dei sistemi di tracciamento, per trovare potenziale trattamento per le più disparate finalità.

Questa nuova realtà, tutt'altro che virtuale nelle sue ricadute, ha generato da tempo l'esigenza di nuove tutele, quasi che al corpo fisico di ogni individuo si sia affiancato con la rivoluzione digitale una sorta di corpo digitale costituito da infiniti frammenti di noi, informazioni personali in formato digitale[9].

Stefano Rodotà, divenuto primo garante per la protezione dei dati in Italia, giunse prima di altri a invocare quello che egli chiamò «*habeas data*», richiamando significativamente l'antico diritto dell'*habeas corpus*[10].

L'*habeas data* invocato da Stefano Rodotà è infatti discendente diretto di quell'*habeas corpus* – letteralmente: "che tu abbia il (tuo) corpo" – che compare nel diritto inglese già nel XII secolo come prima embrionale garanzia per limitare l'arresto e la prigionia dei sudditi.

L'*habeas corpus* nasce dall'esigenza di tutela del corpo fisico dei sudditi dai soprusi dei potenti[11] ed è considerato il primo nucleo da cui si svilupperanno, nei secoli successivi, tutte le garanzie di libertà del cittadino nei confronti dello Stato, ivi comprese quelle estensioni immateriali dell'individuo oggi consolidate quali il domicilio, la riservatezza delle comunicazioni e in generale il diritto al rispetto della vita privata e familiare contenuto nei trattati internazionali.

---

8. Le riflessioni di Luciano Floridi, filosofo dell'Università di Oxford, sono forse le più lucide e le più utili per comprendere l'impatto di quella che egli individua come la quarta rivoluzione dell'uomo: *Id.*, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Raffaello Cortina Editore, Milano, 2017.

9. Sul tema, rilevante il contributo di Monica Alessia Senor nel volume *Il corpo digitale: natura, informazione, merce*, Giappichelli, Torino, 2011.

10. La relazione al Parlamento di Rodotà quale garante dell'Autorità per la protezione dei dati del 2001 è reperibile *online*: www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3541955. Sul tema, vds. S. Rodotà e M. Tallacchini, *Trattato di Biodiritto – Ambito e Fonti del Biodiritto,* Giuffrè, Milano, 2010.

11. L'*habeas corpus* fu codificato nell'«Habeas Corpus Act» del 1679 da Carlo II d'Inghilterra e fu definitivamente consacrato nel «Bill of Rights» del 1689: sostanzialmente, prevedeva la necessità di un mandato scritto (*writ*) per poter arrestare un suddito della Corona e l'obbligo di presentare fisicamente il soggetto all'autorità costituita. Le assonanze, a distanza di secoli, con il "*search and warrant*" richiesto dalla Suprema corte americana nel 2014 in *Riley c. California* per accedere ai dati dello *smartphone* di un arrestato sono evidenti. La sentenza, che immagina i moderni cellulari come «parti essenziali dell'anatomia umana», è reperibile *online*: www.supreme.justia.com/cases/federal/us/573/13-132.

Immaginare un diritto di *habeas data* che possa oggi costituire la base fondativa dei diritti di libertà della persona nella dimensione immateriale dell'infosfera significa riconoscere l'esistenza di una sorta di corpo digitale: quella parte di noi in formato binario composta dai nostri dati e oggetto oggi di potenziali abusi grazie alle tecnologie digitali.

Il diritto alla protezione dei dati è indubbiamente un primo importante tassello; altri seguiranno, come seguirono all'*habeas corpus*: una tutela costituzionale del domicilio informatico, il diritto all'anonimato in rete o diritti più complessi e incerti, come il diritto alla disconnessione da internet o il diritto di rifiutare implementazioni bio-tecnologiche, per non sacrificare, senza adeguata consapevolezza e senza garanzie, il corpo digitale nella pur legittima ricerca di efficienza e sicurezza del corpo fisico.

3. Proteggere i dati

Il potere generato dall'accesso e dal trattamento di grandi moli di dati personali è in grado di modificare profondamente, nel bene e nel male, i rapporti e le relazioni tra le persone e soprattutto tra i diversi attori sociali: tra consumatori e imprese, che infatti hanno costruito un nuovo paradigma commerciale su dati e profilazione, e tra i cittadini e lo Stato, che anche nelle più avanzate democrazie è inevitabilmente attratto da tecnologie di controllo e sorveglianza, verso nuove "data-crazie". Se infatti il potere informativo generato dalla rivoluzione digitale porta evidenti benefici e può davvero, se non fornire la soluzione per tutti i problemi del mondo, essere di fondamentale aiuto in tutti i processi decisionali, bisogna esser coscienti del fatto che, senza un attento governo della tecnologia e un'adeguata protezione del dato, il passaggio tra il legittimo tracciamento degli infetti in una emergenza sanitaria e la repressione del dissenso o la marginalizzazione e la discriminazione di interi settori della società sulla base di elaborazioni statistiche degli algoritmi, è passaggio breve spesso non più distante di qualche "click" del *mouse*[12].

Il diritto alla protezione dei dati personali nasce, sin dagli anni ottanta dello scorso secolo[13], proprio per governare il potere derivante dal trattamento digitale di grandi moli di dati personali ed è diventato solo recentemente, con l'art. 8 della Carta dei diritti fondamentali dell'Unione europea, diritto fondamentale qui in Europa.

È un diritto indissolubilmente legato alle nuove tecnologie digitali e alla dimensione immateriale, e ha evidentemente un perimetro molto più ampio della semplice tutela della riservatezza o del rispetto di una vita privata che già trovavano, da tempo, pieno riconoscimento nelle costituzioni nazionali e sovranazionali.

È un diritto complesso, che attiene all'identità e alla dignità della persona (al "corpo digitale", appunto) e che nasce come diritto necessariamente flessibile, mediato e bilanciato: l'art. 8 della Carta dei diritti fondamentali dell'Unione europea non conferisce infatti al singolo un diritto sui propri dati personali, non crea una privativa o un diritto assoluto, ma tratteggia unicamente un diritto fondamentale a che quei dati, necessariamente disponibili nell'infosfera ed essenziali per il progresso della società dell'informazione, siano "protetti". La complessa normativa europea e nazionale a protezione dei dati personali regola il "come" possono essere usate, secondo il principio di lealtà, le informazioni personali dei cittadini e detta le regole minute che, in relazione alle diverse finalità (determinate) e ai contesti (la legittima base giuridica), rendono il trattamento conforme ai principi democratici.

La protezione del dato personale è dunque un diritto trasversale, flessibile e dinamico, i cui confini di liceità, a fronte della continua innovazione tecnologica e dei diversi contesti, sono mutevoli, frutto del costante bilanciamento tra le legittime finalità perseguite con il trattamento e gli interessi, i diritti e le libertà fondamentali dell'interessato. Quei confini costituiscono l'argine oltre il quale il potere conferito dalle nuove tecnologie diviene abuso del corpo digitale dei cittadini ed è incompatibile con le nostre società democratiche. Non vi è, infatti, una sola libertà tra quelle sancite dalle nostre costituzioni che non possa esser minata o subdolamente limitata là dove, come negli Stati autoritari, viene negato il diritto alla protezione dei dati personali e si ammettono senza adeguato governo tecnologie di sorveglianza di massa e di profilazione.

Come sottolineato dal Comitato europeo per la protezione dei dati («European Data Protection Board» – EDPB), proprio in relazione all'uso di strumenti per il tracciamento dei contatti nel contesto

12. L'infelice comunicato del commissario capo dello Stato del Minnesota (Usa), che il 30 maggio lasciava ad intendere l'utilizzo delle tecnologie di *contact-tracing* predisposte per la pandemia nelle indagini circa i movimenti di protesta seguiti all'omicidio di George Floyd, seppur frutto di un equivoco, è stato significativo. *Cfr*. www.eff.org/it/deeplinks/2020/06/dont-mix-policing-covid-19-contact-tracing.

13. È del 1981 il Trattato n. 108 del Consiglio d'Europa, «Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale», che nell'Unione europea porterà poi alla direttiva 95/46/CE e infine, dopo il Trattato di Lisbona e la "costituzionalizzazione" del diritto alla protezione dei dati personali, al GDPR e alle varie direttive collegate.

dell'emergenza legata al Covid-19[14], il quadro giuridico in materia di protezione dei dati è stato concepito per essere flessibile e, in quanto tale, è in grado di conseguire una risposta efficace per qualunque finalità, in qualunque contesto, anche in emergenza. Applicare alle tecnologie di tracciamento i principi e le prescrizioni dettate dalla normativa a protezione dei dati personali significa semplicemente trovare il giusto equilibrio tra il contenimento della pandemia e la protezione dei diritti umani e delle libertà fondamentali.

Lo stesso «Regolamento generale sulla protezione dei dati personali» (GDPR), da un lato, contempla espressamente la lotta alle epidemie e le emergenze umanitarie in generale come particolare base giuridica per il trattamento[15]; dall'altro, disciplina minutamente tutte le possibili limitazioni che l'Unione e gli Stati membri possono apportare a obblighi e diritti conferiti agli interessati dal regolamento stesso in caso di «importanti obiettivi di interesse pubblico» in materia di sanità pubblica e sicurezza sociale, prescrivendo misure legislative (dunque democraticamente approvate) e specifici vincoli inderogabili[16]. Nel GDPR, dunque, l'emergenza e l'eccezionalità sono disciplinate e riportate nell'ambito della cornice che delimita il diritto fondamentale alla protezione dei dati personali di cui all'art. 8 della Carta dei diritti fondamentali dell'Unione, che è e rimane un diritto, potremmo dire, geneticamente bilanciato e flessibile.

Se un trattamento massivo di dati personali reso possibile da qualsivoglia tecnologia non è pienamente conforme e aderente ai principi e alle prescrizioni tecniche e normative previste dalla normativa a protezione dei dati, le conseguenze di quel trattamento sui diritti delle persone non potranno mai essere proporzionate e necessarie in uno Stato democratico, quale che sia l'encomiabile finalità perseguita e quale che sia l'emergenza.

Il rispetto del diritto fondamentale alla protezione dei dati personali è il parametro ineludibile, la cartina di tornasole per capire se siamo in grado di utilizzare la tecnologia per proteggerci e migliorare le nostre esistenze all'interno delle democrazie che abbiamo così faticosamente costruito, oppure se, attratti dal potere delle nuove tecnologie costituito dall'accesso ai dati personali della popolazione, l'emergenza diventerà, come accaduto spesso in passato, l'occasione per consolidare o creare nuovi poteri e realizzare una società della sorveglianza che annullerebbe la dignità della persona e svuoterebbe le libertà civili e sociali.

4. Finalità e basi giuridiche: *tracing*, *exposure alert* e controllo delle misure di contenimento

Le tecnologie di cui si discute oggi nei Paesi democratici nell'ambito delle politiche per il contenimento dell'epidemia implicano il trattamento di dati personali per molteplici e tra loro differenti finalità, tutte genericamente ricomprese nel concetto di "tracciamento" dei contatti. In particolare: i) ricostruire i contatti, anche occasionali, avuti da soggetti risultati infetti durante il periodo di incubazione e fornire alle autorità sanitarie informazioni sui possibili contagi; ii) creare sistemi automatizzati di allerta ai cittadini in caso di contatti significativi con soggetti risultati potenzialmente contagiosi; e iii) controllare e verificare specifiche situazioni di isolamento e quarantena imposte o di rispetto di norme di distanziamento sociale.

Distinguere tra le diverse finalità perseguite nel trattamento è essenziale, poiché la finalità del trattamento è uno degli elementi fondanti la valutazione di liceità di qualsivoglia tecnologia basata sui dati. Lo stesso articolo 8 della Carta dei diritti fondamentali UE, al comma 2, individua tre elementi base di liceità del trattamento: i) il principio di lealtà (o di equità: «*processed fairly*» nella versione inglese), ii) la finalità appunto, che deve esser "determinata" e iii) la base giuridica, costituita dal consenso del soggetto interessato o da altro fondamento legittimo previsto dalla legge.

Nelle tecnologie di tracciamento ci cui ci occupiamo sono due le normative europee rilevanti, attuative

14. Vds. le linee-guida 04/2020 sull'uso dei dati di localizzazione e degli strumenti per il tracciamento dei contatti nel contesto dell'emergenza legata al Covid-19, adottate il 21 aprile 2020, www.edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_it.pdf.

15. *Considerando* n. 46 GDPR: «Il trattamento di dati personali dovrebbe essere altresì considerato lecito quando è necessario per proteggere un interesse essenziale per la vita dell'interessato o di un'altra persona fisica. Il trattamento di dati personali fondato sull'interesse vitale di un'altra persona fisica dovrebbe avere luogo in principio unicamente quando il trattamento non può essere manifestamente fondato su un'altra base giuridica. Alcuni tipi di trattamento dei dati personali possono rispondere sia a rilevanti motivi di interesse pubblico sia agli interessi vitali dell'interessato, per esempio se il trattamento è necessario a fini umanitari, tra l'altro per tenere sotto controllo l'evoluzione di epidemie e la loro diffusione o in casi di emergenze umanitarie, in particolare in casi di catastrofi di origine naturale e umana».

16. L'art. 23 GDPR, «Limitazioni», disciplina casi e limiti di ogni intervento derogatorio al GDPR, che deve avvenire per legge e rispondere a specifici requisiti, riportando così ogni possibile eccezione nell'ambito del giusto equilibrio tra interessi e diritti in tensione nel pieno rispetto del diritto fondamentale alla protezione del dato.

di tali principi: il GDPR e, nel caso di utilizzo di dati afferenti il settore delle comunicazioni elettroniche, come nel caso di utilizzo degli "apparecchi terminali" (gli *smartphone*) e dei dati ivi archiviati (come per "Immuni") la più risalente direttiva 2002/58/CE del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (d'ora innanzi "direttiva *e-privacy*").

La finalità del trattamento è sempre centrale, poiché se non ho finalità univoche, determinate ed esplicite (*ex* art. 5, par. 1, lett. *b*, GDPR), non solo sarà impossibile individuare il "come" i dati possano essere usati in maniera aderente al diritto, ma sarà altresì impossibile prevedere e governare le possibili ricadute e i rischi sulle libertà personali dei soggetti coinvolti e dunque bilanciare i diversi diritti in tensione; sarà anche difficile valutare se tali misure saranno efficaci (parametro intimamente legato alla finalità) e dunque se le misure siano necessarie e proporzionate al contesto in una società democratica.

Per ogni determinata finalità sarà, poi, diversa la base giuridica del trattamento e la scelta del tipo di tecnologia da utilizzare per acquisire i dati. Sulla scorta dei principi di minimizzazione, di limitazione della conservazione e di integrità e riservatezza (*ex* art. 5 GDPR), saranno diversi i dati acquisibili, la loro tipologia e la loro possibile o doverosa anonimizzazione o pseudonimizzazione, il tempo di conservazione e le misure di sicurezza.

Alla finalità è dunque legato l'algoritmo che governa il trattamento e ovviamente il tipo di architettura del sistema informativo sottostante.

La protezione del dato nasce (*by design* e *by default* – *ex* art. 25 GDPR) contestualmente alla tecnologia (i due aspetti tecnico e legale, nell'informatica, stanno e cadono insieme perché «code is law», nel mondo dei *byte*[17]) e la finalità perseguita dal trattamento è sempre il primo tassello di un procedimento valutativo complesso. Se la finalità è "mappare" possibili focolai, avrò bisogno dei dati di geo-localizzazione degli infetti, che però, a seconda della base giuridica su cui baso il trattamento e delle modalità di acquisizione, potranno/dovranno essere aggregati e anonimi. Tali dati saranno necessari anche per un'attività di controllo dei vincoli di quarantena o isolamento, ma ovviamente nel caso i dati non possono essere anonimi e la base giuridica del trattamento sarà diversa, legata alla prevenzione e repressione di misure restrittive; se la finalità è invece solo individuare possibili contatti interpersonali, a rischio saranno utili solo dati di prossimità, ad esempio tra dispositivi (come per "Immuni"), e non i dati di geo-localizzazione, e i dati potranno essere anonimi; ma se debbo allertare possibili contagiati o monitorarne la loro sintomatologia, i dati non potranno più essere dati anonimi, ma potranno (e dovranno) al più essere pseudonimizzati, per garantire integrità e riservatezza, in particolare per i dati sanitari.

Insomma, ogni variabile nei fini si traduce in differenti prescrizioni normative e in diverse tecnologie e differenti "righe" di codice informatico, e ogni piccola variazione nell'interfaccia tra i diversi sistemi informatici coinvolti nel trattamento e tra applicazione ed utente ha conseguenze molto concrete sulla sicurezza del dato e sulla sua protezione, e dunque sulla vita (reale e quotidiana) delle persone.

5. Tracciamento digitale di prossimità

Da inizio pandemia, diverse soluzioni tecnologiche di "*digital proximity tracking*", ovvero di tracciamento digitale di prossimità, sono state proposte da imprese, gruppi di ricerca e da diversi governi: a norma dei regolamenti sanitari internazionali[18], al manifestarsi di una pandemia, tutti gli Stati membri dell'Organizzazione mondiale della sanità sono tenuti a sviluppare sistemi di sorveglianza per monitorare la malattia e tentare di interrompere il contagio attraverso attività di tracciamento degli infetti. L'occasione per implementare misure di sorveglianza di massa era ed è perfetta, non solo per gli Stati autoritari.

L'attenzione si è subito focalizzata sugli *smartphone* che, come scrisse alcuni anni fa la Corte suprema americana[19], sono ormai da considerare come una parte anatomica essenziale del corpo umano. I nostri cellulari sono ricchi di sensori digitali, sono diffusi in tutto il mondo e consentono di penetrare nella vita delle persone con una efficienza senza precedenti.

Sono dotati di tecnologia *gps* per la geo-localizzazione e, con più ampio margine, grazie alla mappatura delle celle di rete, possono essere utilizzati per

17. «Code is law», «il codice [informatico] è legge», è una delle grandi intuizioni di Lawrence Lessig, tra i primi ad affrontare sul finire del secolo scorso il complesso rapporto tra tecnologia e diritto alla Harvard University. *cfr*. *Id*., *Code is law. On Libery in Cyberspace*, in *Harvard Magazine*, 1° gennaio 2000, www.harvardmagazine.com/2000/01/code-is-law-html.

18. Oms, *International health regulations*, Ginevra, 2005 (seconda ed.), https://apps.who.int/iris/bitstream/handle/10665/43883/9789241580410_eng.pdf?sequence=1.

19. Nel 2014, nella Sentenza *Riley c. California*, i giudici della Corte suprema americana scrivono: «I moderni cellulari sono oggi così presenti e pervasivi nella vita quotidiana che il proverbiale visitatore da Marte potrebbe ritenerli una fondamentale caratteristica dell'anatomia umana» (*cfr*. www.supreme.justia.com/cases/federal/us/573/13-132).

tracciare un singolo utente o mappare la concentrazione di persone in determinati luoghi; inoltre, con la diversa tecnologia *Bluetooth L.E.* ("*Low Energy*") ogni dispositivo può comunicare con i dispositivi che si trovano nel raggio di alcuni metri e scambiarsi informazioni. Se due persone dotate di cellulare abilitato alla trasmissione *bluetooth* rimangono vicine per un certo tempo, i due dispositivi si parlano e possono memorizzare reciprocamente, a determinate condizioni di distanza e tempo di esposizione, un numero identificativo trasmesso dall'interlocutore, consentendo di ricostruire *a posteriori* i "contatti stretti", potenzialmente infettivi.

Nei Paesi dove la protezione del dato non ha ancora ricevuto riconoscimento e dove riservatezza e tutela della vita privata sono considerati diritti deboli e recessivi, o dove semplicemente lo Stato ha colto l'occasione per implementare misure generalizzate di controllo, le soluzioni tecnologiche hanno immediatamente combinato le due tecnologie con sistemi di tracciamento granulare della popolazione per noi inammissibili[20].

Nell'Unione europea, l'utilizzo di dati (metadati) delle comunicazioni elettroniche e l'accesso ad apparecchi terminali degli utenti, gli *smartphone*, trova un significativo ostacolo, più che nel GDPR, nella vecchia "direttiva *e-privacy*", che da un lato limita fortemente l'uso dei metadati delle comunicazioni (tra cui la geo-localizzazione attraverso l'ubicazione delle celle di connessione)[21] e dall'altro inibisce l'archiviazione e l'accesso a dati e informazioni memorizzate sugli apparecchi terminali degli utenti, limitando tale attività al solo consenso espresso dell'utente[22].

Le deroghe a questa ferrea disciplina a tutela della riservatezza delle comunicazioni previste dall'art. 15 dir. 2002/58/CE non contemplano esigenze di salute pubblica[23]; vi è, nella tutela della riservatezza delle comunicazioni della direttiva *e-privacy*, minor flessibilità rispetto alla normativa generale a tutela della protezione dei dati *ex* art 23 GDPR.

Inoltre, l'utilizzo di dati di geo-localizzazione per attività di mero tracciamento dei contatti di prossimità, oltre a vincoli legislativi giustificati dall'invasività particolare di tali informazioni, presenta ulteriori limiti tecnologici: la tracciabilità con le celle telefoniche è imprecisa e non consente di valutare la distanza tra le persone e, dunque, di valutare la reale pericolosità di un contatto a fini di contagio. Non dissimili problemi ha il *gps*, teoricamente più preciso, che non funziona in spazi chiusi o angusti e la cui attivazione sugli *smartphone* genera problemi di consumo energetico rilevanti.

Se la finalità è rintracciare i contatti a rischio contagio di soggetti risultati infetti per interrompere la catena di diffusione, raccogliere dati di geo-localizzazione tramite lo *smartphone* violerebbe tanto la direttiva *e-privacy* (in caso di mancato consenso all'accesso a monte)[24] quanto, e in ogni caso, il principio di minimizzazione previsto dal GDPR, poiché tali dati non sono adeguati né pertinenti (art. 5, lett. *c*, GDPR) per la specifica finalità di prossimità perseguita.

Per queste ragioni, la tecnologia *Bluetooth L.E.* è la tecnologia utilizzata praticamente da tutte le *app* realizzate dai vari governi europei, compresa la *app* italiana "Immuni".

6. "Immuni"

Senza scendere in particolari tecnici, l'architettura di queste applicazioni basate su tecnologia *Bluetooth L.E.* può variare significativamente in ragione di molteplici parametri di programmazione (*code is law*, "il codice è legge"), in particolare in relazione al tipo di identificativo trasmesso tra i vari dispositivi, al tempo di conservazione, alle modalità di comunicazione e, soprattutto, al luogo in cui avviene l'elaborazione algoritmica che determinerà la segnalazione di allarme.

È su tale ultimo aspetto, sintetizzabile nella scelta tra sistemi centralizzati o sistemi decentralizzati (anche qui con mille varabili tra gli estremi), che si è sviluppato il dibattito più vivace.

Trasferire tramite la *app* tutti i vari identificativi, anche se anonimi o pseudonimizzati, su di un

20. La Norvegia, che non fa parte dell'Ue ma risulta fortemente integrata nei principi fondamentali con l'Unione, ha implementato una *app*, "Smittestopp", che combinava le due tecnologie *gps* e *bluetooth*. L'Autorità norvegese per la protezione del dato ha fermato l'uso di tale applicazione per l'eccessiva invasività della stessa: *cfr*. www.fhi.no/en/news/2020/niph-stops-collection-of-personal-data-in-smittestopp.

21. Art. 6 dir. 2002/58/CE.

22. Art. 5, comma 3, dir. 2002/58/CE: è proprio dall'art. 5, comma 3, della direttiva *e-privacy* che discende il requisito, allo stato insuperabile, della volontarietà dell'utilizzo di applicazioni come "Immuni" che attraverso la rete archiviano e accedono a informazioni contenute sull'apparecchio terminale.

23. Art. 15 dir. 2002/58/CE: deroghe sono previste solo se «la misura, necessaria opportuna e proporzionata all'interno di una società democratica, è finalizzata per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica o la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica».

24. Sul punto, le linee-guida emesse dall'EDPB ai punti 12 e 13 (*cfr*. nota 14) sono invero poco chiare, quasi che il Comitato abbia lasciato aperta una possibile interpretazione più flessibile, che consenta un domani agli Stati di poter superare, per ragioni di sanità pubblica, il vincolo del consenso all'accesso a metadati e dispositivi.

server centrale ed elaborare lì tramite algoritmo gli accoppiamenti tra infetti e interlocutori a rischio, per poi scegliere chi avvisare, conferisce ovviamente un maggior controllo al "titolare" del trattamento, ma presenta inevitabilmente variabili di rischio quanto a sicurezza del *database* e a possibili utilizzi ultronei del grafo sociale che può ricavarsi. Inoltre, se la *app* dovesse in futuro svolgere altre funzioni più o meno dichiarate o semplicemente essere in grado di determinare, sulla base ad esempio dell'indirizzo IP di connessione, la localizzazione dei vari contatti, sarebbe molto facile (ri)identificare granularmente i rapporti interpersonali di buona parte della popolazione; in ultimo, è noto in informatica che ogni *database* connesso in rete, soprattutto se molto ricco di informazioni, per quanto protetto è a rischio di attacchi e tentativi di *hacking*, e ovviamente più dati sono concentrati in un unico *server*, più rilevante sarà il danno in caso di *data breach*.

Per ovviare a queste e ad altre vulnerabilità sono state implementate, prima da un consorzio pan-europeo denominato DP-3T poi, con un'iniziativa congiunta, da due colossi come Google e Apple, soluzioni "decentralizzate" ove il sistema di allerta viene gestito in locale, sul singolo dispositivo dalla *app* stessa, senza necessità di caricare su unico *server* tutti gli identificativi dei contatti. In questa soluzione l'autorità statuale titolare del trattamento non conosce nulla dei singoli soggetti che hanno scaricato la *app*, non ha la possibilità di ricostruire e "vedere" il grafo delle relazioni, e di fatto non tratta alcun dato personale al di fuori di quelli dei soggetti risultati positivi (che già tratta per ragioni di cura o per il tradizionale *tracing* tramite interviste). Il soggetto risultato positivo viene autorizzato dall'operatore sanitario (a seguito di verifica di positività) a rendere visibili a tutte le *app* i codici identificativi anonimi trasmessi nel periodo di incubazione così che la stessa *app* dei singoli interlocutori, verificata l'eventuale coincidenza dei codici memorizzati in locale, possa segnalare l'avvenuto "contatto stretto".

È questa, in estrema sintesi, la tecnologia di "Immuni" che senza alcun dubbio, con la pubblicazione del codice aperto[25] e l'adozione del protocollo definito da Apple e Google, risulta pienamente aderente alla normativa a tutela dei dati personali, alle linee-guida emesse dal EDPB (*cfr*. la nota 14) e alle raccomandazioni di cui alla comunicazione della Commissione europea del 17 aprile 2020[26].

Ai sensi dell'art. 5, comma 3, direttiva *e-privacy* (art. 122, commi 1 e 2-*bis*, cod. *privacy*) l'installazione della *app* sul dispositivo è necessariamente volontaria, subordinata al consenso dell'utente e sempre revocabile, come volontario è l'utilizzo della stessa e dunque, in caso di accertata positività al virus, sarà il soggetto a decidere in autonomia se condividere i propri codici anonimi e consentire l'allerta dei soggetti con cui ha avuto contatti.

La base giuridica del trattamento dei dati personali, che non è il consenso per l'installazione sullo *smartphone* della *app* – che, come detto, ha diversi presupposti normativi –, è correttamente individuata ai sensi dell'art. 6, par. 1, lett. *e*, GDPR nella «esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento»; ai sensi del comma 3 del medesimo articolo, tale base giuridica si fonda sul dl n. 28/2020, che individua all'art. 6 la finalità del trattamento, il titolare del trattamento e le condizioni generali di liceità.

Dalla visione del codice pubblicato in ogni sua parte dal Governo sulla piattaforma "*GhitHub*"[27], l'algoritmo di "Immuni" risulta oggettivamente ben costruito, sicuro, e supporta un trattamento pienamente conforme ai principi dettati dal GDPR.

Insomma, "Immuni" è un'applicazione aderente alle linee-guida, alle raccomandazioni e alle migliori prassi pubblicate dal Comitato europeo per la protezione dei dati.

Rimane una domanda: "Immuni" è utile per il contenimento della pandemia?

7. I limiti del soluzionismo digitale

Un efficiente sistema di tracciamento (digitale, con algoritmi che analizzano i nostri dati, o analogico, con interviste e indagini interpersonali) è solo uno dei tasselli necessari per il contenimento delle epidemie sintetizzati nelle ben note "3T": i) "*test*", "testare"; ii) "*treat*", "trattare/isolare"; iii) "*trace*", "tracciare". Il tracciamento è attività efficace unicamente se vi sono a monte massive e rapide capacità diagnostiche (*test*: i tanto invocati tamponi di questa pandemia) e un'organizzazione efficiente nel trattamento dei casi infetti e, ovviamente, dei soggetti allertati (*treat*: isolamento e, possibilmente, cura).

Qualsiasi soluzione tecnologica di *tracing*, anche più invasiva dei sistemi di semplice allerta predisposti

25. www.github.com/immuni-app.

26. Comunicazione della Commissione 2020/C 124 I/01: «Orientamenti sulle app a sostegno della lotta alla pandemia di covid-19 relativamente alla protezione dei dati», www.eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020XC0417%2808%29.

27. www.github.com/immuni-app.

dalla maggior parte dei Paesi europei, rischia di esser inefficace nel contenimento della pandemia se non inserita in una chiara riorganizzazione dell'intero sistema sanitario e soprattutto dei servizi di assistenza ai soggetti segnalati dall'algoritmo.

Vi sono però due ulteriori criticità, tra loro connesse e correlate, che temo minino in radice l'efficacia delle *app* di allerta all'esposizione adottate. La prima è costituita dai limiti propri della tecnologia utilizzata: da più parti sono stati avanzati molti dubbi, e non c'è ad oggi alcun dato certo, sulla necessaria correlazione tra la vicinanza degli *smartphone* calcolata con *bluetooth* e reali rischi di trasmissione del virus. Il *bluetooth* utilizza le onde radio e ottenere una misurazione affidabile del segnale per determinare la distanza tra i dispositivi e, in relazione al tempo di esposizione, qualificare una prossimità (dei dispositivi) come "contatto stretto" a rischio reale di infezione (delle persone) è operazione tecnicamente molto complessa e incerta, perché influenzata da molteplici fattori ambientali incontrollabili. Le onde radio possono essere interrotte da oggetti che si frappongono tra i due dispositivi e l'*app* non sarà mai in grado di calcolare se una parete di plexiglas, un muro o banalmente una mascherina sono presenti tra i due interlocutori. I falsi positivi e quelli negativi possono essere molto elevati, e questa incertezza influenza l'altro fattore di criticità che è il fattore umano. Affinché la *app* possa essere efficace, è necessario che un'alta percentuale della popolazione acconsenta e la utilizzi[28]. Ma la condizione di fiducia che indurrà la popolazione a scaricare la *app*, fugati tutti i dubbi sulla *privacy* e sulla tutela dei dati come nel caso di "Immuni", dipende essa stessa dall'efficacia della *app* e, soprattutto, dall'efficacia del sistema complessivo di tracciamento: le persone scaricheranno la *app* se ogni allerta avrà un chiaro significato a cui seguono chiare procedure sanitarie di tutela della persona allertata. Ricevere una notifica di rischio al Covid-19 non è fatto irrilevante, anche psicologicamente, e ciò che accade dopo l'allerta deve esser definito e regolamentato ufficialmente.

E su questo punto si inserisce la fragilità più evidente del sistema.

La circolare del Ministero della salute del 29 maggio 2020, «*Ricerca e gestione dei contatti di casi COVID-19 (Contact tracing) ed App Immuni*»[29], non contempla l'allerta notificata dalla *app* "Immuni" tra i casi di "contatto stretto" da cui discendono chiare indicazioni di isolamento e/o *test*. La definizione di "contatto stretto" nella circolare sembrerebbe derivare solo dalla tradizionale procedura di tracciamento svolta tramite intervista dell'infetto.

La scelta può trovare ragione sia nell'incertezza tecnica propria delle notifiche automatizzate di cui si è appena detto, sia dal vincolo normativo discendente dall'art. 22 GDPR[30]: la sola elaborazione algoritmica di prossimità dei dispositivi non può, in effetti, determinare effetti giuridici vincolanti sulle persone.

Chi riceve un'allerta dalla *app* "Immuni" viene semplicemente invitato a contattare il medico di base, ma ci si chiede quale valutazione dovrebbe fare l'operatore sanitario a fronte di un soggetto asintomatico che ha ricevuto una notifica "cieca", che non fornisce alcuna indicazione per identificare il luogo, il tempo e soprattutto la persona fonte di potenziale infezione. Al momento, secondo la predetta circolare, l'esecuzione di *test* diagnostici è riservata ai "contatti stretti" dell'infetto ricavati dalla tradizionale attività di tracciamento e solo all'insorgere dei sintomi. Dunque, la conseguenza dell'allerta di "Immuni" è un semplice invito a contattare un operatore sanitario che non avrà elementi significativi per compiere alcuna valutazione, né sarà possibile per l'operatore sanitario ricondurre e collegare quella notifica a un'attività di tracciamento "tradizionale" in atto sul soggetto infetto che ha dato il via alle notifiche, che è e resta anonimo.

Il significato di quell'allerta è davvero incerto. Cosa accade se un soggetto allertato si reca al lavoro e infetta i colleghi dell'ufficio? Potrà tale condotta, l'aver ignorato la notifica di esposizione, costituire un elemento di colpa generica, di imprudenza o di negligenza? Come gestiranno i casi di allerta i medici di base a fronte di soggetti asintomatici? Sono domande tutt'altro che irrilevanti, che incidono su quella fiducia che dovrebbe sorreggere un ampio utilizzo dell'applicazione da parte della popolazione.

Ciò che è certo è che, in tutti gli Stati in cui sono state adottate tecnologie di *contact tracing* più o meno invasive, la percentuale di utilizzo è al momento bassa e l'efficacia di tali tecnologie per il contenimento del virus assai dubbia: in Francia la *app* "StopCovid" è stata

28. La percentuale, spesso citata, del 60% della popolazione deriva da uno studio dell'Università di Oxford reperibile *online* al seguente indirizzo: www.coronavirus-fraser-group.org/for-media.

29. La circolare è reperibile *online*: www.trovanorme.salute.gov.it/norme/renderNormsanPdf?anno=2020&codLeg=74178&parte=1%20&serie=null.

30. Art. 22 GDPR: «Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione. 1. L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona».

scaricata dal 3% della popolazione, in Italia siamo a circa 4 milioni di *download*, e anche in un Paese altamente digitalizzato e socialmente avvezzo alle tecnologie di stato come Singapore l'utilizzo si è fermato al 35% della popolazione.

Ma ciò che rileva è che, indipendentemente da quanto sofisticate e invasive siano le tecnologie adottate, in tutti i Paesi è emersa chiara la convinzione che, allo stato, nulla può sostituire nel contenimento di una crisi sanitaria l'interazione umana tradizionale. Due dei Paesi di maggior successo nel contenere l'epidemia da Covid-19, la Corea del Sud e Taiwan, si sono affidati in larga misura a eserciti di persone reali che eseguono una capillare attività di tracciamento dei contatti sul campo, con gli infetti, eseguendo milioni di *test* diagnostici.

Vivian Balakrishnan, il ministro responsabile della «Smart Nation Initiative» di Singapore, ha dichiarato recentemente in un *post* su *Facebook*: «Secondo me, il rintracciamento dei contatti rimane uno sforzo umano che richiede giudizi umani. La tecnologia è solo un integratore, non un sostituto per gli umani. Bisogna affidare informazioni ai tracciatori umani durante questa crisi. Forse il mio passato medico mi fa sentire fortemente che i pazienti dovrebbero essere informati di una diagnosi, conseguenze e opzioni da un essere umano – e non da una macchina»[31].

Decisamente, almeno per ora, non saranno le tecnologie digitali a risolvere l'attuale crisi sanitaria e, in generale, i problemi del mondo.

31. https://www.facebook.com/Vivian.Balakrishnan.Sg/posts/several-people-have-asked-why-we-are-not-using-the-exposure-notification-system-/10156889801466207/.