LE TECNOLOGIE, LA PROTEZIONE DEI DATI E L'EMERGENZA CORONAVIRUS: RAPPORTO TRA IL POSSIBILE E IL LEGALMENTE CONSENTITO

Francesco Paolo Micozzi[*]

**** 15 marzo 2020 ****

Nel periodo a cavallo tra il 2019 e il 2020 ha iniziato a diffondersi, a livello mondiale, la pandemia di COVID-19 (causata dal virus SARS-CoV-2). La pandemia in questione, la cui diffusione avrebbe avuto origine nella città cinese di Wuhan, arriva in Italia verso la fine del mese di gennaio 2020 con una tale viralità da imporre al Governo l'adozione una serie di misure emergenziali (racchiuse nei provvedimenti D.L. nn. 6, 9 e 14 del 2020 e DPCM del 1, 4, 8, 9 e 11 marzo 2020, reperibili nel *Dossier Coronavirus Italia* su *biordiritto.org*). Non sono mancati, col moltiplicarsi delle notizie sull'incremento esponenziale dell'epidemia, episodi di minacce, lesioni e atti discriminatori ai danni di persone dai tratti asiatici che, per gli aggressori, erano sicuro indizio di veicolo d'infezione e per ciò solo sufficienti a certificarne la qualità di moderni untori, giustificandone, infine, la persecuzione.

Episodi tragicamente simili a quelli descritti dal Manzoni ne *I promessi sposi* (cap. XXXII), in cui ai tempi della peste a Milano (1630) le persone si convincevano dell'esistenza stessa degli untori e delle loro "unzioni" di "*muraglie, porte d'edifizi pubblici e usci di case*"; credenza rapidamente diffusa attraverso il chiacchiericcio. E il chiacchiericcio popolare, intriso d'isteria collettiva determinata dalla paura, si trasformava quasi inevitabilmente in conferma delle unzioni ("*il sentire faceva l'effetto del vedere*") e nella conseguente caccia all'untore, ossia a coloro che "*gli animi, sempre più amareggiati da' mali*" riconoscevano come la causa del diffondersi della peste e contro i quali la gente potesse "*far valere le sue vendette*" ("*ogni atto poteva dar gelosia; e la gelosia diveniva facilmente certezza, la certezza furore*"). Analoghi episodi di violenza, (forse meno cruenti) si sono registrati nella cronaca di quasi quattro secoli dopo, a seguito della diffusione del COVID-19.

Certo, durante la pandemia descritta dal Manzoni non si disponeva delle conoscenze della medicina moderna (e al più si faceva ricorso a soluzioni pseudoscientifiche commiste a riti

[*]*Avvocato e Professore a contratto di Informatica Giuridica, Università degli Studi di Perugia*. Mail: *francescopaolo.micozzi@unipg.it*. Il contributo è stato accettato per la pubblicazione nell'ambito della call *Diritto, diritti ed emergenza ai tempi del Coronavirus*, sul n. 2/2020 di BioLaw Journal – Rivista di BioDiritto.

religiosi o, nelle migliori ipotesi, alle decameroniane "quarantene"), né ci si interrogava sul bilanciamento degli interessi nella tutela dei dati personali. Occorreranno, infatti, quasi tre secoli perché Samuel Warren e Louis Brandeis, dalle pagine della Harward Law Review, presentino al mondo "*The right to privacy*" (1890).

Tuttavia, ai giorni nostri, benché il concetto di privacy e la rilevanza fondamentale della protezione dei dati personali siano largamente riconosciuti, è comunque possibile costatare come la stessa disciplina di tutela sia percepita e abbia un impatto differenziato in ragione del contesto democratico, culturale e giuridico raggiunto nelle differenti aree del pianeta. La diffusione di una pandemia – che è di per sé situazione eccezionale – può, pertanto, incidere nel bilanciamento tra i valori da tutelare, fino a lasciar insinuare la suggestione che la diffusione di informazioni personali degli "untori", nel supremo interesse alla salute pubblica, sia qualcosa di ragionevole. Difficilmente ci si interroga, con altrettanta determinazione, sulla mancanza di evidenze circa la prevalenza dei benefici offerti dalla diffusione dei dati personali dei contagiati, in termini di contenimento della diffusione virale, né sulle conseguenze negative che i soggetti i cui dati personali venissero diffusi andrebbero a scontare.

Secondo quanto riportato dalla BBC, ad esempio, la Corea del Sud, al fine di monitorare la diffusione del COVID-19 avrebbe messo in atto per la prima volta le misure straordinarie già varate nel 2015, in occasione della diffusione di un'altra epidemia di coronavirus simile alla SARS (MERS-CoV – Middle East Respiratory Syndrome). Con i "messaggi di orientamento sulla sicurezza", realizzati con un invio massivo di SMS da parte del Governo sudcoreano, si è voluto informare la popolazione sulle misure igieniche raccomandate, comprendendo anche l'indicazione dei luoghi frequentati dalle persone risultate infette. A ciò si aggiunge la possibilità di tracciare le persone contagiate attraverso i dati GPS, le informazioni di riconoscimento facciale provenienti dalle telecamere di sorveglianza o le informazioni bancarie circa le transazioni con carte di credito. Si ottiene così un monitoraggio costante, in tempo reale, estremamente parcellizzato e su larga scala dell'intera popolazione, che viene giustificato con l'interesse "supremo" della salvaguardia della salute collettiva. Il contenuto degli SMS inviati ai cittadini, inoltre, è arricchito da dettagli del seguente tenore "*Un quarantatreenne residente nel distretto di X è risultato positivo al Coronavirus. Egli si trovava nel distretto di Y, dove lavora, e frequentava un corso sulle molestie sessuali. Ha contratto il virus dal suo istruttore*". Nel corpo dell'SMS non sono dunque indicate le generalità della persona asseritamente contagiata, ma ne sono diffusi il genere, l'età e un codice di riferimento della segnalazione, insieme a un

link attraverso cui seguire gli spostamenti del soggetto segnalato. Tuttavia, attraverso una ricerca online sul codice della segnalazione si possono recuperare ulteriori dettagli della persona contagiata, tra i quali, "volto", "fotografie", "familiari" o, anche, elementi relativi a eventuali ipotesi di "adulterio" (ad esempio per essersi recati, in determinate ore del giorno, in ambienti nei quali, notoriamente, si pratica la prostituzione).

Tale attività, definita di "contact tracing", ossia di tracciamento dei soggetti incontrati e dei luoghi frequentati dalle persone contagiate mira, in sostanza, ad osservare la propagazione del virus sul territorio, e, allo stato attuale della tecnica, potrebbe astrattamente essere attuato tramite dati GPS, installazione di applicazioni da parte delle autorità sui dispositivi dei cittadini, analisi delle transazioni con carte di credito o altri mezzi di pagamento, analisi dei dati di geolocalizzazione a disposizione dei gestori di telefonia mobile, o attraverso l'uso dei Big Data (dati provenienti, ad esempio, da società produttrici di *device* "smart", dati delle tessere fedeltà dei market, dati di rilevamento delle targhe, dati provenienti da telecamere con riconoscimento facciale…). Dal *mashup* di questa enorme mole di informazioni personali provenienti da diverse fonti, è possibile disegnare un quadro assai dettagliato circa gli spostamenti di un'intera popolazione e dei singoli soggetti contagiati, oltre a quelli entrati con loro in contatto.

Un sistema come quello descritto è certamente più efficiente di quello demandato alle autodichiarazioni degli individui (previsto invece dai provvedimenti d'urgenza emanati dal Governo italiano): l'analisi automatizzata dei dati incrociati consentirebbe, anche grazie all'ausilio di algoritmi di Intelligenza Artificiale, di intervenire con azioni di prevenzione e contenimento più rapide e mirate. Ma l'interrogativo è un altro: per quale ragione si propone di utilizzare le nuove tecnologie per contrastare l'epidemia? Perché i mezzi a disposizione – sia quelli di prevenzione (come i dispositivi personali di protezione) che quelli di diagnosi (come i tamponi) e cura (tra cui i respiratori artificiali) – sono limitati e un quadro più chiaro e dettagliato della situazione potrebbe consentire agli operatori di non agire alla cieca e ottimizzare gli interventi.

Occorre, a questo punto, comprendere se e come nel nostro Paese possano essere predisposte misure tecniche analoghe.

Il presupposto è il necessario bilanciamento tra diritti di pari rilevanza: da una parte la libertà personale e il diritto alla protezione dei dati personali, dall'altra la protezione della salute individuale e pubblica.

L'Europa conosce, ormai da qualche anno, un Regolamento sulla protezione dei dati personali

(Regolamento UE 2016/679, comunemente indicato con l'acronimo GDPR) che definisce la tutela dei dati personali come contributo «alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche» (considerando 2). Al contempo, pur riconoscendo (cons. 1) la tutela delle persone fisiche con riguardo al trattamento dei dati di carattere personale come diritto fondamentale ai sensi della Carta dei diritti fondamentali dell'Unione europea (art. 8, par. 1) e del Trattato sul funzionamento dell'Unione europea (art. 16, par. 1), esclude che si tratti di una "prerogativa assoluta" (cons. 4) e afferma, anzi, che tale tutela vada considerata alla luce della sua funzione sociale e contemperata con altri diritti fondamentali.

La protezione dei dati personali, in situazioni emergenziali come quelle attuali, caratterizzate anche dal diffuso timore del contagio di un male inarrestabile, viene messa a dura prova. E ciò in considerazione del crescente (come si vedrà, falso) convincimento, che la riduzione delle tutele garantite (anche) agli "untori" sia un male necessario, ma minore rispetto a quello cui è esposta la salute pubblica.

Come contemperare, allora, la protezione dei dati personali con l'interesse pubblico a che il virus non si propaghi oltre la soglia di reazione del sistema sanitario?

L'art. 6 del GDPR contempla, tra le diverse basi giuridiche di legittimità del trattamento, sia la necessità di salvaguardare gli interessi vitali dell'interessato o di un'altra persona fisica, sia la necessità di realizzare un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui sia investito il titolare (bisogna focalizzare l'attenzione sul fatto che tale trattamento debba essere "necessario" agli scopi menzionati). Il considerando 46 del GDPR, oltretutto, prevede la possibilità che alcune finalità, quale quella di tenere sotto controllo l'evoluzione di epidemie e la loro diffusione, possano trovare il giusto inquadramento in entrambe le basi giuridiche appena menzionate.

Ogni informazione relativa allo stato di salute di una persona fisica rappresenta un dato appartenente alle "categorie particolari" di cui all'art. 9 del GDPR, che detta il divieto generale di trattare tale categoria di dati personali salvo che non ricorrano alcune specifiche eccezioni. Tra queste ultime è ricompreso il trattamento di dati relativi a una persona fisica (e specificamente al suo stato di salute) necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero", sempreché siano predisposte (dalle norme dell'UE o dello Stato) delle "misure appropriate e

specifiche per tutelare i diritti e le libertà dell'interessato (quale, ad esempio, il segreto professionale). Ciò significa, ad esempio, che – come esplicitato dal considerando 54 – il trattamento di categorie particolari di dati, in presenza di tali basi giuridiche, può prescindere dal consenso dell'interessato (che rappresenta un'altra delle basi giuridiche previste dall'art. 6 GDPR).

Con riferimento alla situazione della pandemia COVID-19, inoltre, è rilevante l'art. 14 del D.L. 9 marzo 2020, n. 14 (disposizioni sul trattamento dei dati personali nel contesto emergenziale), che prevede misure specifiche in tema di trattamento dei dati personali (efficaci fino al termine dell'attuale stato d'emergenza). In specie, nel rispetto degli artt. 9, par. 2, lett. g), h) e i), e 10 del GDPR, determinati soggetti impegnati nel contrasto all'emergenza COVID-19 (tra i quali il Servizio nazionale di protezione civile, gli uffici del Ministero della salute e dell'Istituto Superiore di Sanità, le strutture pubbliche e private che operano nell'ambito del Servizio sanitario nazionale) possono trattare anche dati personali di cui agli artt. 9 e 10 del GDPR, che risultino necessari all'espletamento delle funzioni loro attribuite nella gestione dell'emergenza. Non si realizza pertanto, né si poteva realizzare, una deroga alle disposizioni del GDPR (fonte gerarchicamente sovraordinata), ma si definiscono i ruoli e i compiti nel trattamento dei dati (in particolare quelli relativi allo stato di salute) per finalità di tutela della salute pubblica. Si prevede inoltre (al secondo comma dell'art. 14) la possibilità che tali dati personali vengano "comunicati" anche a soggetti diversi e, ancora, che vengano "diffusi" dati personali diversi da quelli previsti negli artt. 9 e 10 GDPR, ma unicamente nelle ipotesi in cui la comunicazione o la diffusione risultino indispensabili alla gestione dell'emergenza in atto. Rilevante è, infine, l'ultimo comma, a mente del quale una volta cessato lo stato d'emergenza devono essere adottate misure idonee a ricondurre i trattamenti di dati personali effettuati nel contesto dell'emergenza, all'ambito delle ordinarie competenze e delle regole che disciplinano i trattamenti di dati personali.

Nello stesso senso si dirige il comunicato del Garante privacy (del 2 marzo 2020) nel ricordare ai soggetti pubblici e privati che le attività di accertamento e la raccolta di informazioni relative ai sintomi tipici del Coronavirus e alle informazioni sui recenti spostamenti di ogni individuo spettano agli operatori sanitari e al sistema attivato dalla protezione civile, che sono gli organi deputati a garantire il rispetto delle regole di sanità pubblica recentemente adottate. Ad ulteriore conferma, si segnala il Comunicato del Comitato europeo per la protezione dei dati personali del 16 marzo 2020 (http://bit.ly/2UcFfDh).

I termini "necessario" e "indispensabile", contemplati dalle norme europee e nazionali appena menzionate, sono un chiaro richiamo ai principi regolatori di ogni trattamento dei dati personali e, in particolare, al principio di "minimizzazione", in base al quale possono essere trattati unicamente i dati personali adeguati, pertinenti e limitati a quanto necessario a soddisfare le finalità per le quali sono trattati.

Nella vigenza di tale quadro normativo, è agevole comprendere che uno scenario come quello descritto dalla Corea del Sud (in cui si è assistito a una diffusione di dati relativi allo stato di salute, sebbene pseudonimizzati) non sarebbe giustificato nemmeno dalla normativa d'emergenza contenuta nel DL 14/2020, proprio perché nel "modello" sudcoreano non sarebbe rispettato il principio di minimizzazione, che non potrebbe essere "silenziato" da una fonte gerarchicamente subordinata al GDPR. Inoltre, il DL 14/2020 nulla prevede in relazione al trattamento dei dati relativi all'ubicazione di utenti o abbonati di reti pubbliche di comunicazione o di servizi di comunicazione elettronica accessibili al pubblico. In assenza di una specifica previsione, il trattamento dei dati di ubicazione è soggetto alla disciplina di cui all'art. 126 D.Lgs. 196/03 (in conformità a quanto previsto dall'art. 9 della c.d. Direttiva e-privacy, 2002/58/CE). Le eventuali disposizioni interne, derogatorie alle limitazioni a tali trattamenti, possono essere introdotte – ai sensi dell'art. 15 della Direttiva e-Privacy – qualora tale restrizione costituisca una misura necessaria, opportuna e proporzionata all'interno di una società democratica.

Potrebbero piuttosto utilmente essere adottate modalità di informazione del pubblico in modo da evitare la diffusione di dati personali identificativi, relativi allo stato di salute, ma comunque "allertando" le persone potenzialmente contagiate, e permettere loro di acquisire informazioni più dettagliate da parte delle autorità preposte.

Non si ravvisano – quantomeno nella vigenza del DL 14/2020 – ostacoli particolari a che i già menzionati soggetti, deputati alla gestione dell'emergenza, possano trattare i dati personali dei contagiati (anche provenienti da terze parti) al fine di effettuare attività di *contact tracing* utile a delineare i contorni del fenomeno virale. Ovviamente, una volta cessata l'emergenza (e raggiunta, quindi, la finalità del trattamento), la mole di informazioni raccolte non potrà – in assenza di ulteriore base giuridica che ne giustifichi il trattamento – essere "convertita" al soddisfacimento di finalità ulteriori. Al contrario, una volta anonimizzate, le informazioni potrebbero essere riutilizzate a fini di ricerca e per qualsiasi finalità lecita, e senza limiti temporali. È fuori di dubbio, infatti, che il dato informativo, una volta reso anonimo – ossia quel

dato che, passando attraverso un procedimento di anonimizzazione, non possa essere in alcun modo ricondotto a una singola persona fisica – non rientrerebbe nell'ambito applicativo del GDPR e il suo riuso non creerebbe problemi di sorta.

Occorre evitare, però, di confondere il concetto di dato anonimo sia con quello di dato pseudonimo (che, in quanto dato personale, resta disciplinato dal GDPR) che con quello di Open Data (o "dato aperto", così come definito dall'art. 1, co. 1, lett. l-ter del D.Lgs. 82/2005 e che potrebbe anche racchiudere anche dati personali), che, infine, con quello di Big Data (con il quale si indica, solitamente, la raccolta di una mole enorme di dati informativi eterogenei per fonte, formato e contenuti).

Una delle soluzioni proposte nel 2015, proprio dal Garante europeo per la protezione dei dati personali (con riferimento al caso del virus Ebola), allo scopo di prevedere la diffusione del contagio sul territorio e di informare tempestivamente i gruppi di persone eventualmente e direttamente coinvolte, è rappresentata proprio dall'uso dei Big Data (o "megadati"). Con questo termine ci "*si riferisce alla crescita esponenziale sia della disponibilità sia dell'utilizzo automatizzato di informazioni, indicando enormi serie di dati digitali detenuti da società, governi e altre organizzazioni di grandi dimensioni, successivamente analizzati in modo estensivo attraverso algoritmi informatici*" (parere 3/2013, Article 29 WP). Al contemperamento degli interessi del singolo con quelli della collettività si dirige la strategia dell'UE di promozione della progettazione e dello sviluppo di "*algoritmi che mascherano l'identità e aggregano i dati al fine di proteggere le persone, sfruttando al contempo il potere predittivo degli stessi dati*" (EDPS, Parere 4/2015, "*Verso una nuova etica digitale*").

In conclusione, la disciplina sulla protezione dei dati personali non rappresenta un ostacolo all'efficientamento della prevenzione e contrasto dell'epidemia ma, al contempo, non ammette un'abdicazione alla tutela dei diritti fondamentali. Pertanto, nel perseguimento delle finalità preventive e di contenimento dell'epidemia dovranno, anzitutto, preferirsi le soluzioni tecnologiche che impieghino dati anonimi. L'uso, invece, di dati personali sarà ammissibile – in una situazione di emergenza che, comunque, come può determinare la compressione di altre libertà fondamentali (quale quella alla libera circolazione delle persone) potrà determinare anche la compressione del diritto alla protezione dei dati personali – purché le misure predisposte siano proporzionate alle esigenze di contrasto e siano circoscritte al tempo dell'emergenza. La questione, quindi, non può ridursi all'alternativa dell'utilizzo o meno delle tecnologie disponibili, ma va sapientemente condotta, con l'utilizzo delle tecnologie e dei dati

personali, nel rispetto dei principi generali in materia di protezione dei dati personali.