NOMOS
Le attualità nel diritto

Quadrimestrale di teoria generale, diritto pubblico comparato e storia costituzionale

Martina Cardone* e Marco Cecili**

Osservazioni sulla disciplina in materia di tutela dei dati personali in tempi di Covid-19. L'Italia e i modelli sudcoreano, israeliano e cinese: opzioni a confronto[1]***

SOMMARIO: 1. La normativa emergenziale e il diritto alla riservatezza dei dati personali. - 2. Il necessario bilanciamento tra diritti. - 3. Tecnologia: una strategia di uscita dal Covid-19? Uno sguardo a tre modelli extraeuropei. – 4. Conclusioni: l'innovazione tecnologica e i limiti invalicabili dello Stato di diritto.

1. La normativa emergenziale e il diritto alla riservatezza dei dati personali

Come ha lucidamente colto Giuseppe Ugo Rescigno non ci sono casi di scuola ed esiste un «dovere dei giuristi di rispondere ai quesiti giuridicamente possibili»[2]. Avendo a mente questo pensiero, possiamo cogliere i motivi per i quali l'emergenza ha sempre affascinato il mondo giuridico[3]. In tal senso, è ancor più evidente perché la crisi sanitaria in atto, dovuta al

* Dottoranda di ricerca in Diritto e Impresa presso la LUISS Guido Carli.
** Dottorando di ricerca in Diritto Pubblico presso l'Università di Roma -Tor Vergata.

[1] La materia è in continua e rapidissima evoluzione. Il contributo analizza quanto accaduto fino all'8 maggio 2020. Il presente scritto è frutto della stretta cooperazione tra i due autori: ad ogni modo, i paragrafi 1 e 2 sono stati redatti da Marco Cecili, mentre il paragrafo 3 da Martina Cardone. Le conclusioni sono frutto di riflessioni condivise.

*** Contributo sottoposto a *double blind peer review*.

[2] G.U. RESCIGNO, *Il "caso Mancuso", ovvero della inesistenza dei casi di scuola, ovvero ancora del dovere dei giuristi di rispondere ai quesiti giuridicamente possibili*, in *Diritto pubblico*, n. 1/1996, pp. 235-242.

[3] Si pensi, ad esempio, al concetto di *stato d'eccezione* e alle riflessioni di Carl Schmitt (*Teologia politica* e *Legalità e legittimità*, in IDEM, *Le categorie del 'politico'*, a cura di G. Miglio, P. Schiera, il Mulino, 1972; *La ditttura*, Settimo sigillo, 2006), Bruce Ackerman (*La Costituzione dell'emergenza*, Meltemi, 2005), Max Weber (*Economia e società*, Donzelli, 1961) e Giorgio Agamben (*Stato di eccezione*, Bollati Boringhieri, 2003). In questo scritto non si vuole considerare quello attuale come uno stato d'eccezione, che permette un'aggressione profondissima delle tutele costituzionali (fra tutti, F. RIMOLI, *Stato di eccezione e trasformazioni costituzionali: l'enigma costituente*, in *Associazionedeicostituzionalisti.it*, 30 aprile 2007). La domanda che dovrebbe animare ogni riflessione sul tema è se la Costituzione sia capace di "isolare e contenere" il fenomeno emergenziale (sul tema G. DE MINICO, *Costituzione ed emergenza*, in *Osservatoriosullefonti.it*, n. 2/2018). Allargando lo sguardo in chiave comparata si può notare che la Costituzione spagnola prevede diversi regimi emergenziali, come ad esempio l'*estado de alarma ex* art. 116, comma 2 (per A.M. GARCÍA CUADRADO, *El ordenamiento constitucional*, Editorial Club Universitario, 2002, p. 192 l'*estado de excepción* permette una sospensione *erga omnes* dei diritti, mentre con quello de *alarma* si realizzerebbe una limitazione meno pesante). Anche l'ordinamento francese fa convivere l'*état d'urgence*

ISSN 2279-7238

diffondersi della pandemia del Covid-19, e le politiche del Governo per combatterne la diffusione stiano facendo sorgere molteplici riflessioni giuridiche[4].

Il Governo, prima attraverso Decreti del Presidente del Consiglio dei Ministri e poi con decreti-legge[5], ha di fatto "sospeso" alcuni diritti previsti in Costituzione[6] ed intaccato anche buona parte dei "nuovi diritti", tra cui la *privacy* e la riservatezza dei dati[7]. Su quest'aspetto, forse, si gioca uno dei punti nevralgici della tenuta delle garanzie minime che uno stato liberal-democratico deve mantenere.

Concentrando lo sguardo sulla riservatezza dei dati, è opportuno segnalare che la Carta dei diritti fondamentali dell'Unione europea (c.d. Carta di Nizza), oltre a prevedere l'inviolabilità della dignità umana, della libertà, dell'uguaglianza e della solidarietà, sancisce anche il diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni (art. 7) e il diritto di ogni persona alla protezione dei dati di carattere personale che la riguardano (art. 8[8]).

(istituito in Francia con la Legge n. 385 del 3 aprile 1955), lo stato d' assedio (previsto dall'articolo 36 della Costituzione) e i poteri eccezionali *ex* art. 16 della Costituzione (cfr. G. TAFFINI, *Stato di diritto e stato d'emergenza in Francia*, in *Questione Giustizia*, 25 marzo 2016). Per una lettura dell'ordinamento tedesco, cfr. A. JAKAB, *German Constitutional Law and Doctrine on State of Emergency – Paradigms and Dilemmas of a Traditional (Continental) Discourse*, in *German Law Journal*, n. 5/2006, pp. 453-477. Per una ricostruzione generale e comparata sullo stato di emergenza si veda A. PIZZORUSSO, *Emergenza (stato di)*, in *Enciclopedia delle scienze sociali,* 1993 (ora in *Treccani.it*).

Si segnalano, legati specificatamente al coronavirus, A. RUGGERI, *Il coronavirus, la sofferta tenuta dell'assetto istituzionale e la crisi palese, ormai endemica, del sistema delle fonti*, in Consulta-Online, n. 1/2020, p. 203, nt. 1; V. BALDINI, *Emergenza costituzionale e costituzione dell'emergenza. Brevi riflessioni (e parziali) di teoria del diritto*, in *Dirittifondamentali.it*, n. 1/2020.

[4] Per un primo commento, si veda M. CAVINO, *Covid-19. Una prima lettura dei provvedimenti adottati dal governo*, in *Federalismi.it - Osservatorio emergenza Covid-19,* 18 marzo 2020*;* I.A. NICOTRA, *L'epidemia da Covid-19 e il tempo della responsabilità*, in *Diritti Regionali*, 23 marzo 2020.

[5] Una delle questioni che più hanno animato il dibattito pubblico è il ruolo giocato dal Presidente del Consiglio. Dal punto di vista strettamente giuridico, l'analisi deve concentrarsi sulla natura degli atti adottati dall'Esecutivo per affrontare la crisi (F. PETRINI, *Emergenza epidemiologica Covid19, decretazione d'urgenza e costituzione in senso materiale*, in *Nomos - Le attualità del diritto*, n. 1/2020; C. PINELLI, *Il precario assetto delle fonti impiegate nell'emergenza sanitaria e gli squilibrati rapporti fra Stato e Regioni*, in *Rassegna Astrid*, n. 5/2020). La posizione centrale del Governo è stata immediatamente chiara con l'emanazione decreto-legge del 23 febbraio 2020, n. 6, che ha demandato (apparentemente con una c.d. delega in bianco) alla normazione secondaria la potestà di affrontare la gestione dell'emergenza sanitaria. L'effettiva emanazione di DPCM e di decreti ministeriali ha fatto immediatamente sorgere dubbi sull'idoneità di questi strumenti a "sospendere" alcuni diritti costituzionali (sul tema, fra tutti, M. CAVINO, *op.cit.*; E. RAFFIOTTA, *Sulla legittimità dei provvedimenti del Governo a contrasto dell'emergenza virale da coronavirus*, in *Biolaw Journal Instant Forum - Diritto, diritti ed emergenza ai tempi del Coronavirus*, 18 marzo 2020; M. LUCIANI, *Il sistema delle fonti del diritto alla prova dell'emergenza*, in *Rivista Aic*, n. 2/2020). Il decreto-legge 25 marzo 2020, n. 19 sembrerebbe porsi l'obiettivo di conferire "*forza di legge*" alle misure precedentemente adottate al fine di evitare ulteriori polemiche sulla violazione delle riserve di legge previste in Costituzione.

[6] Le misure disposte per il contenimento e gestione dell'emergenza epidemiologica da Covid-19 comportano la limitazione di diversi diritti costituzionali, primo tra tutti la libertà di movimento e vanno a determinare importanti ricadute in una molteplicità di settori, dalla libertà di circolazione (art. 16 Cost.) al diritto al lavoro (artt. 4 e 35 ss. Cost.), fino a interessare l'esercizio delle attività di culto (art. 19 Cost.), il diritto di voto (art. 48 Cost.), la libertà di riunione (art. 17 Cost.), il diritto all'istruzione (art. 33 Cost.) e il diritto d'iniziativa economica (art. 41 Cost.). Tra i molti commenti, si veda S. PRISCO, F. ABBONDANTE, *I diritti al tempo del coronavirus. Un dialogo*, in *Federalismi.it - Osservatorio emergenza Covid-19*, 24 marzo 2020.

[7] Sul tema c'è una letteratura molto vasta. Tra i primi ad affrontare il tema, si veda: A. BALDASSARRE, *Privacy e Costituzione. L'esperienza statunitense*, Bulzoni, 1974; A. PIZZORUSSO, *Sul diritto alla riservatezza nella Costituzione italiana*, in *Prassi e teoria*, 1976, pp. 33 ss.; V. FROSINI, *La protezione della riservatezza nella società informatica*, in *Informatica e diritto*, n. 1/1981, pp. 5-14; S. RODOTÀ, *Privacy e costruzione della sfera privata*, in *Politica del diritto*, n. 4/1991, p 521 ss.

[8] L'articolo 8 recita: «*Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.*

Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica.

Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente».

ISSN 2279-7238

Seguendo questi principi, il Regolamento Europeo per la protezione dei dati personali (di seguito GDPR**)** all'art. 9 disciplina la tutela dei dati c.d. sensibilissimi. Come è noto la disposizione vieta il trattamento di **«***dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona***»**[9]. Il dato relativo alla salute è definito come quello riguardante «*la salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute*»[10].

Le misure adottate dal Governo si indirizzano principalmente verso un "nuovo" trattamento dei dati sensibilissimi da parte del Servizio Sanitario Nazionale e della Protezione civile per combattere la diffusione della pandemia. Questi dati, invero, sono al centro delle disposizioni normative da ultimo emanate e già nell'art. 5 dell'ordinanza del Dipartimento di Protezione civile del 3 febbraio 2020, n. 630 si consente che «*nell'ambito dell'attuazione delle attività di protezione civile connesse allo svolgimento delle attività di cui alla presente ordinanza, allo scopo di assicurare la più efficace gestione dei flussi e dell'interscambio di dati personali, i soggetti operanti nel Servizio nazionale di protezione civile* [e gli uffici del Ministero della salute e dell'Istituto Superiore di Sanità, le strutture pubbliche e private che operano nell'ambito del SSN ed in generale tutti i soggetti coinvolti nella emergenza come elencati al DPMC del 5 marzo 2020[11]] *possono realizzare trattamenti, ivi compresa la comunicazione tra loro, dei dati personali* […] *fino al 30 luglio 2020*»[12].

Il comma 2 del medesimo articolo specifica, inoltre, che la comunicazione dei dati personali a soggetti pubblici e privati, diversi da quelli indicati al comma 1, è effettuata nei casi in cui essa risulti indispensabile, mentre nel comma 3 si rinvia al rispetto dei principi generali dell'art. 5 del GDPR[13].

Con il decreto-legge 9 marzo 2020, n. 14 il Governo ha adottato nuove "*Disposizioni urgenti per il potenziamento del Servizio sanitario nazionale in relazione all'emergenza COVID-19***".** L'art. 14 dispone che fino al termine dello stato di emergenza si può effettuare, tra le altre cose, l'interscambio dei dati personali che risultino necessari all'espletamento delle funzioni attribuite nell'ambito dell'emergenza determinata dal diffondersi del virus. Tale operazione, come sottolineato, deve avvenire da parte dei soggetti operanti nel Servizio nazionale di protezione civile (e gli stessi previsti nell'ordinanza 630/2020) «*per motivi di interesse pubblico nel settore della sanità pubblica e, in particolare* […] *anche allo scopo di assicurare la più efficace gestione dei flussi e dell'interscambio di dati personali*»[14]. L'obiettivo della disposizione è quello di realizzare uno scambio di informazioni al fine di garantire una adeguata protezione dall'emergenza attraverso misure di profilassi, nonché assicurare la diagnosi e

[9] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE, Articolo 9, par. 1.

[10] GDPR, Articolo 4, definizione 15.

[11] Soggetti ai quali la stessa ordinanza rinvia.

[12] Dipartimento della Protezione civile, Ordinanza 3 febbraio 2020, n. 630 ("*Primi interventi urgenti di protezione civile in relazione all'emergenza relativa al rischio sanitario connesso all'insorgenza di patologie derivanti da agenti virali trasmissibili*"), art. 5, comma 1. Su questo atto era stato chiesto un parere al Garante per la protezione dei dati personali, emesso il 2 febbraio 2020.

[13] L'art. 5, par. 1, del GDPR afferma i principi di: liceità, correttezza e trasparenza (lett. a), limitazione delle finalità (lett. b), minimizzazione dei dati (lett. c), esattezza (lett. d), limitazione della conservazione (lett. e), integrità e riservatezza (lett. f). Il comma 2 prevede che «*il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo ("responsabilizzazione")*».

È importante segnalare che l'art. 5, comma 4, dell'ordinanza 630/2020 Dip. Prot. civ. permette che le autorizzazioni *ex* art. 2-*quaterdecies* del D. Lgs. 196/2003 possano essere conferite con modalità semplificate, ed anche oralmente.

[14] Decreto-legge 9 marzo 2020, n. 14 ("*Disposizioni urgenti per il potenziamento del Servizio sanitario nazionale in relazione all'emergenza COVID-19*"), art. 14, comma 1.

ISSN 2279-7238

l'assistenza sanitaria dei contagiati ovvero la gestione emergenziale da parte del Servizio Sanitario Nazionale.

Per quanto riguarda gli obblighi intercorrenti tra privati, è necessario tenere in considerazione il Protocollo siglato il 14 marzo tra sindacati e associazioni di categoria, sulla sicurezza nei luoghi di lavoro[15]. Il punto 2 del Protocollo prevede che al momento dell'accesso i lavoratori possono essere sottoposti in tempo reale al controllo della temperatura corporea. Come specificato in una nota, è bene evidenziare che «*la rilevanza della temperatura corporea costituisce un trattamento di dati personali e, pertanto, deve avvenire ai sensi della disciplina privacy vigente*» e non bisogna registrare il dato[16]. La stessa nota suggerisce la modalità con cui svolgere l'operazione: il dato va conservato solo se ciò risulti necessario a documentare le ragioni che hanno impedito l'accesso ai locali aziendali.

Il Governo ha adottato, infine, il decreto-legge 17 marzo 2020, n. 18 ("*Misure di potenziamento del Servizio sanitario nazionale e di sostegno economico per famiglie, lavoratori e imprese connesse all'emergenza epidemiologica da COVID-19*"). Con l'art. 76 del d.l. viene istituito un «*gruppo di supporto digitale alla Presidenza del Consiglio dei Ministri per l'attuazione delle misure di contrasto all'emergenza COVID-19*» e viene previsto che, al fine di dare concreta attuazione alle misure adottate per il contrasto e il contenimento del diffondersi del virus, «*il Presidente del Consiglio dei Ministri, o il Ministro delegato, fino al 31 dicembre 2020 si avvale di un contingente di esperti, in possesso di specifica ed elevata competenza nello studio, supporto, sviluppo e gestione di processi di trasformazione tecnologica, con particolare riferimento alla introduzione di soluzioni di innovazione tecnologica e di digitalizzazione della pubblica amministrazione*»[17].

In ultimo, il decreto-legge 30 aprile 2020, n. 28 ("*Misure urgenti per la funzionalità dei sistemi di intercettazioni di conversazioni e comunicazioni, ulteriori misure urgenti in materia di ordinamento penitenziario, nonché disposizioni integrative e di coordinamento in materia di giustizia civile, amministrativa e contabile e misure urgenti per l'introduzione del sistema di allerta Covid-19*") ha previsto la prima disciplina organica del *contact tracing*[18]. È stata istituita una piattaforma unica nazionale per la gestione del sistema di allerta dei soggetti che, a tal fine, hanno installato, su base volontaria, un'apposita applicazione (c.d. Immuni) sui dispositivi di telefonia mobile, al solo fine di allertare le persone che siano entrate in contatto stretto con soggetti risultati positivi e tutelarne la salute attraverso le previste misure di prevenzione[19].

Il titolare del trattamento è individuato nel Ministero della Salute, che si raccorda con i soggetti operanti nel Servizio nazionale della protezione civile e le strutture operanti nel Servizio Sanitario

[15] Protocollo condiviso di regolamentazione delle misure per il contrasto e il contenimento della diffusione del virus Covid-19 negli ambienti di lavoro, 14 marzo.

[16] *Ivi*, punto 2, nota 1.

[17] Decreto-legge 17 marzo 2020, n. 18 ("*Misure di potenziamento del Servizio sanitario nazionale e di sostegno economico per famiglie, lavoratori e imprese connesse all'emergenza epidemiologica da COVID-19*"), art. 76, comma 1. La lista dei membri nominati è stata resa nota in data 31 marzo 2020, dal Ministro per l'Innovazione. In data 29 aprile 2020 state rese pubbliche le relazioni finali dei gruppi di lavoro (disponibili su www.innovazione.gov.it).

[18] Al Garante per la protezione dei dati personali è stato chiesto dal Governo un parere prima dell'emanazione del decreto-legge (cfr. *Parere sulla proposta normativa per la previsione di una applicazione volta al tracciamento dei contagi da COVID-19 - 29 aprile 2020*, in *garanteprivacy.it*, 29 aprile 2020).

[19] Art. 6, decreto-legge 30 aprile 2020, n. 28 ("*Misure urgenti per la funzionalità dei sistemi di intercettazioni di conversazioni e comunicazioni, ulteriori misure urgenti in materia di ordinamento penitenziario, nonché disposizioni integrative e di coordinamento in materia di giustizia civile, amministrativa e contabile e misure urgenti per l'introduzione del sistema di allerta Covid-19*"). Inoltre, con l'ordinanza 16 aprile 2020, n. 10 il Commissario straordinario per l'attuazione e il coordinamento delle misure occorrenti il contenimento e contrasto dell'emergenza epidemiologica COVID-19 (istituito con l'art. 122 del decreto-legge 17 marzo 2020, n. 18) ha autorizzato la stipula del contratto di concessione gratuita della licenza d'uso sul software di *contact tracing* e di appalto di servizio gratuito con la società Bending Spoons S.p.a.

ISSN 2279-7238

Nazionale per gli ulteriori adempimenti necessari alla gestione del sistema di allerta e per l'adozione di correlate misure di sanità pubblica e di cura[20].

Il Ministero della salute, all'esito di una valutazione di impatto, costantemente aggiornata, adotta misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato ai rischi elevati per i diritti e le libertà degli interessati, ed è previsto un parere del Garante per la protezione dei dati personali[21].

Nel merito, si richiede che gli utenti ricevano, prima dell'attivazione dell'applicazione, informazioni chiare e trasparenti al fine di raggiungere una piena consapevolezza, in particolare, sulle finalità e sulle operazioni di trattamento, sulle tecniche di pseudoanonimizzazione utilizzate e sui tempi di conservazione dei dati[22]. Inoltre, i dati personali raccolti devono essere esclusivamente quelli necessari ad avvisare gli utenti dell'applicazione di rientrare tra i "contatti stretti" di altri utenti accertati positivi al COVID-19, nonché ad agevolare l'eventuale adozione di misure di assistenza sanitaria in favore degli stessi soggetti[23]. Il trattamento effettuato per allertare i contatti deve basarsi sul trattamento di dati, ma resi anonimi oppure, ove ciò non sia possibile, pseudoanonimizzati. È stata esclusa in ogni caso la geolocalizzazione dei singoli utenti[24]. L'applicazione deve garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento nonché misure adeguate ad evitare il rischio di "reidentificazione" degli interessati cui si riferiscono i dati pseudoanonimizzati oggetto di trattamento[25].

Infine, i dati relativi ai contatti stretti devono essere conservati, anche nei dispositivi mobili degli utenti, per il periodo strettamente necessario al trattamento, la cui durata è stabilita dal Ministero della salute e i dati sono cancellati in modo automatico alla scadenza del termine[26].

Il mancato utilizzo dell'applicazione non comporta alcuna conseguenza [27]. L'utilizzo dell'applicazione e della piattaforma, nonché ogni trattamento di dati personali, durerà fino alla data di cessazione dello stato di emergenza e comunque non oltre il 31 dicembre 2020. Entro questa data tutti i dati personali trattati in questa fase devono essere cancellati o resi definitivamente anonimi[28].

L'ultimo decreto è il cuore della disciplina governativa in materia di *contact tracing*. È indubbio che l'utilizzo della tecnologia possa migliorare la qualità delle nostre vite, fino addirittura a proteggerle. Tuttavia, è fondamentale che gli strumenti utilizzati siano ispirati ai principi generali di trasparenza e proporzionalità[29].

[20] Art. 6, comma 1, decreto-legge 30 aprile 2020, n. 28. I dati raccolti attraverso l'applicazione possono utilizzati per soli fini di sanità pubblica, profilassi, statistici o di ricerca scientifica.
[21] Art. 6, comma 2, decreto-legge 30 aprile 2020, n. 28.
[22] Art. 6, comma 2, lett. a), decreto-legge 30 aprile 2020, n. 28.
[23] Art. 6, comma 2, lett. b), decreto-legge 30 aprile 2020, n. 28.
[24] Art. 6, comma 2, lett. c), decreto-legge 30 aprile 2020, n. 28.
[25] Art. 6, comma 2, lett. d), decreto-legge 30 aprile 2020, n. 28.
[26] Art. 6, comma 2, lett. e), decreto-legge 30 aprile 2020, n. 28.
[27] Art. 6, comma 4, decreto-legge 30 aprile 2020, n. 28.
[28] Art. 6, comma 6, decreto-legge 30 aprile 2020, n. 28.
[29] Come affermato anche da Antonello Soro, presidente dell'Autorità garante per la protezione dei dati personali, nell'intervista "*In uno stato d'eccezione è lecito rinunciare a qualche libertà. Ma il nostro modello non potrà mai essere la Cina*", pubblicata il 19 marzo 2020 in *garanteprivacy.it*.

ISSN 2279-7238

2. Il necessario bilanciamento tra diritti

Dalla disamina normativa sin ora svolta, emergono chiaramente limitazioni alla tutela prevista *ex* art. 9 GDPR e quindi al diritto alla riservatezza. Sembra ragionevole domandarsi, dunque, se sia possibile derogare alla disciplina sul trattamento dei dati personali.

Lo stesso GDPR riconosce la non assolutezza della tutela dei dati personali, prevedendo numerose deroghe, condizionate però a determinate situazioni, tra cui quelle legate a motivi di salute.

Come già visto, l'art. 9 del GDPR vieta il trattamento di dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona. Tale divieto però, come esplicitato dal paragrafo 2 del medesimo articolo, non si applica se il trattamento sia necessario per motivi di interesse pubblico nel settore della sanità, *«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, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale»*[30]. L'art. 23 del GDPR chiede che tale limitazione rispetti il nucleo dei diritti e delle libertà fondamentali di uno stato democratico e sia una misura necessaria e proporzionata per salvaguardare in particolare un rilevante interesse di sanità pubblica e sicurezza sociale (lett. e).

La lettura dell'intero GDPR rafforza l'idea della non assolutezza del diritto alla riservatezza dei dati, anche di quelli sensibilissimi. Innanzitutto, il *Considerando 46* garantisce la liceità del trattamento di dati personali quando sia necessario per 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*»[31]. Il *Considerando* 52 prevede poi che è possibile derogare al divieto di trattare i dati *ex* art. 9 GDPR se ciò avviene nell'interesse pubblico e in particolare per finalità di sicurezza sanitaria, controllo e allerta, prevenzione o per il controllo di malattie trasmissibili e altre minacce gravi alla salute. Come sottolinea il *Considerando*, «*tale deroga può avere luogo per finalità inerenti alla salute, compresa la sanità pubblica e la gestione dei servizi di assistenza sanitaria, soprattutto al fine di assicurare la qualità e l'economicità delle procedure per soddisfare le richieste di prestazioni e servizi nell'ambito del regime di assicurazione sanitaria, o a fini di archiviazione nel pubblico interesse o di ricerca scientifica o storica o a fini statistici*»[32]. Ed ancora, come specifica il *Considerando* 53, le categorie particolari di dati personali *ex* art. 9 GDPR dovrebbero essere trattate solo per finalità connesse alla salute e a beneficio delle persone e dell'intera società. Tale deroga riguarda in particolare la gestione dei servizi e sistemi di assistenza sanitaria o sociale, compreso il trattamento di tali dati *«da parte della dirigenza*

[30] Il GDRP prevede deroghe all'art, 9, comma 2, lettere g (motivi di interesse pubblico), h (medicina preventiva) e i (motivi di interesse pubblico nel settore della sanità pubblica). Anche la normativa interna riconosce la possibilità di deroghe, ad esempio il D. Lgs. 196/2003, articolo 2-*sexies*, comma 2, lettere t (attività amministrative e certificatorie correlate a quelle di diagnosi, assistenza o terapia sanitaria o sociale) ed u (compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario, nonché compiti di igiene e sicurezza sui luoghi di lavoro e sicurezza e salute della popolazione, protezione civile, salvaguardia della vita e incolumità fisica).

[31] GDPR, *Considerando* 46.

[32] GDPR, *Considerando* 52.

ISSN 2279-7238

e delle autorità sanitarie nazionali centrali a fini di controllo della qualità, informazione sulla gestione e supervisione nazionale e locale generale del sistema di assistenza sanitaria o sociale, nonché per garantire la continuità dell'assistenza sanitaria o sociale e dell'assistenza sanitaria transfrontaliera o per finalità di sicurezza sanitaria, controllo e allerta o a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in base al diritto dell'Unione o nazionale che deve perseguire un obiettivo di interesse pubblico, nonché per studi svolti nel pubblico interesse nell'ambito della sanità pubblica»[33]. Il *Considerando* 112, infine, prevede che le deroghe dovrebbero in particolare valere per i trasferimenti di dati richiesti e necessari per importanti motivi di interesse pubblico, ed è esplicitato come esempio quello di scambio internazionale di dati servizi competenti in materia di sicurezza sociale o sanità pubblica, ad esempio in caso di ricerca di contatti per malattie contagiose[34].

Dalla lettura delle disposizioni sin ora citate, si può evincere che la disciplina italiana non si ponga in contrasto con la normativa europea e le limitazioni sembrano essere ragionevoli e proporzionali.

Quest'ultimo concetto, però, merita un'ulteriore riflessione. La giurisprudenza europea ha importato da quella tedesca un controllo di proporzionalità incentrato su tre fasi di giudizio[35] ed è, quindi, opportuno verificare se le misure previste superino questi "test", già largamente usati dalla Corte di Giustizia[36]. Il primo controllo che va effettuato è quello dell'idoneità (*Geeignetheit*), che riguarda la relazione positiva tra strumenti legislativi e indirizzi politici. In altre parole, bisogna domandarsi se la disciplina sia idonea a raggiungere l'obbiettivo prefissato. La risposta è positiva. La *ratio* della normativa derogatoria in tema di dati personali mira a garantire la maggior diffusione di informazioni e dati per poter svolgere un'adeguata profilassi della pandemia. Il secondo test da effettuare è quello della necessità (*Notwendigkeit*) o regola del "mezzo più mite". Il controllo presuppone il positivo riscontro della idoneità dell'atto: un mezzo "inutile" o inidoneo, infatti, non potrà di certo essere necessario. Più precisamente, il controllo di necessità postula l'esistenza di diverse misure legislative, parimenti idonee alla realizzazione di un interesse statale, individuando quello capace di realizzare l'obiettivo e che leda il meno possibile gli altri diritti e interessi coinvolti. Nel caso in esame, le misure adottate in materia di trattamento di dati personali non appaiono eccessivamente invasive. La terza, e forse più delicata fase, è quella del bilanciamento di interessi e valori (*Abwägung*), che deve cogliere il valore politico e sociale sotteso alla normativa, per sottoporlo poi ad una valutazione costi-benefici e commisurare i sacrifici patiti dal singolo con i vantaggi conseguiti dalla collettività. Tale controllo è ancor più importante quando vengono in rilievo i diritti fondamentali e la loro limitazione deve avvenire nella misura considerata opportuna. Invero, il perseguimento di un ragionevole interesse generale, in altri termini, deve essere considerato motivo sufficiente per giustificare una limitazione nell'esercizio di libertà costituzionali, con la specificazione che, dinanzi a questi interventi limitativi, il diritto fondamentale va difeso da imposizioni "eccessivamente onerose". Nel caso di specie, i valori in gioco sono il diritto alla salute

[33] GDPR, *Considerando* 54. Inoltre, è importante ricordare che lo stesso *Considerando* ammette che il trattamento di categorie particolari di dati personali può essere necessario per motivi di interesse pubblico nei settori della sanità pubblica, senza il consenso dell'interessato.

[34] GDPR, *Considerando* 112.

[35] Per un'approfondita ricostruzione si veda, G. SCACCIA, *Il controllo di proporzionalità della legge in Germania, in Annuario di diritto tedesco*, 2002, pp. 409-445.

[36] Tra i molti, G. SCACCIA, *Proporzionalità e bilanciamento tra diritti nella giurisprudenza delle corti europee*, in *Rivista AIC*, n. 3/2017. In lingua inglese, *ex plurimis* N. EMILIOU, *The principle of proportionality in European law: a comparative study*, Kluwer Law International, 1996; K. SHAW, *The Court of Justice of the European Union: Subsidiary and Proportionality*, Brill Nijhoff, 2018.

ISSN 2279-7238

e quello alla riservatezza. La normativa emergenziale ha consentito agli enti impegnati a far fronte alla crisi sanitaria di operare trasferimenti di dati tra di loro, senza scopi specifici se non l'emergenza stessa e all'esterno a soggetti pubblici o privati solo ai fini dello svolgimento delle attività connesse alla pandemia. Per comprendere meglio la natura del bilanciamento, può essere d'aiuto la "*Dichiarazione sul trattamento dei dati personali nel contesto dell'epidemia di COVID-19*"[37] del 19 marzo 2020 emessa dal Comitato europeo per la protezione dei dati, la quale afferma che la lotta contro le malattie trasmissibili è un importante obiettivo condiviso da tutte le nazioni e, pertanto, dovrebbe essere sostenuta nel miglior modo possibile.

L'emergenza, infatti, è una condizione giuridica che può legittimare limitazioni delle libertà, a condizione che tali compressioni siano proporzionate e confinate a tale periodo[38], tanto che il GDPR consente, nel contesto di un'epidemia, alle competenti autorità sanitarie pubbliche e ai datori di lavoro di trattare dati personali, anche senza il consenso dei singoli[39].

La legislazione "emergenziale" italiana appare quindi legittima, anche se va specificato (nella normativa di dettaglio) come saranno archiviati e utilizzati i dati raccolti una volta che lo stato di emergenza cesserà[40]. Appare in linea con queste conclusioni il fatto che il legislatore abbia deciso la cancellazione completa dei dati raccolti al di fuori della disciplina "ordinaria", ma andrà ponderato l'eventuale utilizzo che potrebbe essere fatto dei dati in campo scientifico e di ricerca. A tal proposito il decreto-legge 14/2020 prevede che al termine dello stato di emergenza siano adottate le misure idonee per 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*»[41], così come il decreto-legge 28/2020.

Da ciò si può notare che l'invasività delle deroghe previste dalla legislazione italiana in materia di *privacy* non appare intollerabile e che la lesione della sfera privata dei cittadini è limitata, anche se non mancano aspetti di criticità. Infatti, come abbiamo visto, il Governo ha adottato misure di *contact tracing*, anche sulla scorta della Lombardia.

La regione guidata da Attilio Fontana, infatti, in data 30 marzo, ha modificato l'applicazione *AllertaLOM*[42] attraverso la quale si raccolgono i dati di tutti gli utenti che decidono di scaricarla (ad esempio indirizzi IP e codici IMEI identificativi degli *smartphone*)[43]. Inoltre, l'*app* prevede la facoltà

---

[37] European Data Protection Board, *Statement by the EDPB Chair on the processing of personal data in the context of the COVID-19 outbreak*, 16 marzo 2020.

[38] *Ibidem.*

[39] Nel contesto lavorativo, il trattamento dei dati personali può essere necessario per adempiere un obbligo legale al quale è soggetto il datore di lavoro, per esempio in materia di salute e sicurezza sul luogo di lavoro o per il perseguimento di un interesse pubblico come il controllo delle malattie e altre minacce di natura sanitaria. Come analizzato, il Regolamento prevede anche deroghe al divieto di trattamento di talune categorie particolari di dati personali, come i dati sanitari, se ciò è necessario per motivi di interesse pubblico rilevante nel settore della sanità pubblica.

[40] Questo, dal punto di vista teorico, ci porta a un grande problema sotteso alla problematica degli stati di emergenza, che va oltre l'obiettivo di far cessare la situazione emergenziale, ma che è il ripristino dell'ordine precedente. Sul tema, si veda A. CARDONE, *La "normalizzazione" dell'emergenza*, Giappichelli, 2011.

[41] Decreto-legge 9 marzo 2020, n. 14, art. 14, comma 6. Per quanto riguarda i rapporti tra giuslavoristici, il Protocollo stipulato il 14 marzo 2020 individua come durata per la conservazione dei dati il termine dello stato d'emergenza.

[42] *AllertaLOM* è l'applicazione della Protezione civile per la Lombardia, in uso già prima dell'emergenza sanitaria, per ricevere notifiche ed informazioni sulle problematiche del territorio (meteo, rischio neve e valanghe, rischio idrogeologico *etc.*).

[43] Questo sistema sembra trovare una base giuridica nell'art. 126 del D. Lgs. 193/2003 (c.d. Codice Privacy): «*I dati relativi al traffico, riferiti agli utenti o agli abbonati di reti pubbliche di comunicazione o di servizi di comunicazione elettronica accessibili al pubblico, possono essere trattati solo se anonimi o se l'utente o il contraente ha manifestato previamente il proprio consenso, revocabile in ogni momento, e nella misura e per la durata necessari per la fornitura del servizio a valore aggiunto richiesto*».

ISSN 2279-7238

per l'utente di aderire al progetto *CercaCovid*[44], compilando un questionario con il quale sono raccolti dati sullo stato di salute. I dati vengono registrati in forma anonima e la posizione dell'utente è dedotta dal codice di avviamento postale: in tal modo, le risposte non vengono collegate ai dati personali o al numero di telefono. I cittadini non ricevono alcuna indicazione, né risposta in base alle informazioni che hanno inserito, ma contribuiscono a fare chiarezza sulla diffusione del Covid-19.

Il trattamento dei dati delle telecomunicazioni come i dati relativi all'ubicazione deve rispettare le leggi nazionali di attuazione della direttiva 2002/58/CE, relativa alla vita privata e alle comunicazioni elettroniche[45]. Questi dati possono essere utilizzati dall'operatore solo se resi anonimi o con il consenso dei singoli, ma l'articolo 15 della direttiva consente agli Stati membri dell'UE di introdurre misure legislative per salvaguardare la sicurezza pubblica, sempre rispettando i principi di necessarietà, adeguatezza e proporzionalità[46]. È importante, dunque, adottare adeguate misure di sicurezza e riservatezza che garantiscano che i dati personali non siano divulgati a soggetti non autorizzati. Si dovrebbero, infine, documentare in misura adeguata le misure messe in campo per gestire l'attuale emergenza e il relativo processo decisionale.

3. Tecnologia: una strategia di uscita dal Covid-19? Uno sguardo a tre modelli extraeuropei

Da tali riflessioni, si evince la difficoltà di adattare il quadro normativo alla situazione emergenziale. Lo Stato italiano, a dispetto delle deroghe al GDPR, cerca di trovare mezzi idonei per tutelare il diritto alla *privacy* e alla riservatezza dei dati, al fine di evitare una *tirannia* da parte del diritto alla salute[47].

È di chiara evidenza che lo stato di emergenza mette a dura prova la tenuta democratica della maggior parte degli Stati, europei e non. L'emergenza è una condizione giuridica che può legittimare limitazioni delle libertà, le quali devono essere proporzionate e confinate a tale periodo. È innegabile che a fronte di una situazione inaspettata, sia faticoso operare il bilanciamento tra i diritti fondamentali, dove la prevalenza di uno determina compressioni legittime di altri[48].

Il rapporto tra diritti di uguale rilevanza, in particolare il diritto alla protezione dei dati personali e il diritto alla salute, si colloca al centro del dibattito attuale. Lo Stato ha l'obbligo di tutelare la

[44] CercaCovid è un progetto della regione Lombardia che mira a tracciare la mappa del rischio di contagio da parte del virus. Ogni utente compila quotidianamente un questionario (una sorta di *triage*) per evidenziare la comparsa di sintomi e di conseguenza zone e probabilità di diffusione.

[45] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche.

[46] Direttiva 2002/58/CE, art. 15. Come afferma lo *Statement by the EDPB Chair,* questa legislazione eccezionale è possibile **solo se** costituisce una **misura necessaria, adeguata e proporzionata all'interno di una società democratica**. Tali misure devono essere conformi alla Carta dei diritti fondamentali e alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali. Inoltre, esse sono **soggette al controllo giurisdizionale della Corte di giustizia dell'Unione europea e della Corte europea dei diritti dell'uomo.** In presenza di situazioni di emergenza, le misure in questione devono essere rigorosamente limitate alla durata dell'emergenza.

[47] Il termine *tirannia dei valori* deriva dalle riflessioni DI C. SCHMITT, *La tirannia dei valori. Riflessioni di un giurista sulla filosofia dei valori, Adelphi*, 2008. Tale pensiero è stato alla base della celebre sentenza della Corte costituzionale n. 85 del 2013.

[48] U. ALLEGRETTI, *Il trattamento dell'epidemia di "coronavirus" come problema costituzionale e amministrativo*, in *Forum di Quaderni Costituzionali*, 25 marzo 2020, p. 4.

ISSN 2279-7238

collettività, limitando il contagio e, al contempo, salvaguardare la salute dei singoli individui. Si è iniziato a propendere, dunque, per un possibile uso di sistemi di tracciamento e di raccolta di dati per le finalità di tutela della salute pubblica, diffondendosi sempre più l'idea che sia necessario un salto tecnologico nella lotta al coronavirus. Si va, in questo modo, verso una direzione di maggiore invasività della sfera personale, a detrimento delle conquiste che negli ultimi anni si sono avute in materia di *privacy*.

Il ricorso ai *Big Data*[49] per tracciare i cittadini in quarantena, il controllo rigoroso della diffusione delle informazioni, la sorveglianza degli individui, lo sviluppo di *app* di tracciamento con condivisione dei dati con le diverse autorità, sono ulteriori presidi che i governi scelgono di adottare come misure di contenimento del virus, oltre al distanziamento sociale.

Il problema è che per questa raccolta e analisi di dati occorrono tempo e strumenti adeguati: nel momento storico che stiamo vivendo, infatti, è necessario chiedersi sia fino a quanto uno Stato democratico possa sacrificare alcuni diritti per realizzare una profilassi, anche attraverso l'uso della tecnologia e dei dati personali, sia quanto il diritto alla protezione dei dati personali possa essere soggetto ad una diversa disciplina di tutela in base al contesto democratico, culturale e giuridico[50]. Per questi motivi la scelta comparativa è caduta su tre ordinamenti extraeuropei, che sono anche quelli maggiormente richiamati dalle fonti giornalistiche, dove la concezione dei diritti è molto diversa: Corea del Sud, Israele e Cina.

La Corea del Sud ha messo in atto delle misure straordinarie, già adottate durante l'epidemia Mers del 2015[51], per monitorare la diffusione del Covid-19. Il sistema, attraverso un progetto di "smart city" avviato dal governo centrale[52] nel 2003, di concerto con i Centri di controllo e prevenzione delle malattie infettive (KCDC), mira a raccogliere una quantità enorme di dati, provenienti dai *database* governativi e non solo.

Il Ministero dell'Interno e della Sicurezza sudcoreano, infatti, ha iniziato a tracciare la posizione delle persone contagiate dal virus, autorizzando, per finalità di controllo delle malattie infettive, l'accesso ai dati personali detenuti nei *database* governativi, a quelli delle telecamere posizionate in luoghi pubblici, a quelli derivanti dal tracciamento tramite GPS e a quelli legati alle transazioni con carta di credito. Tali dati vengono pubblicati su un sito *web*[53], nel quale convergono le informazioni sui contagi, i decessi, i guariti e gli spostamenti delle persone risultate positive. Il governo coreano, inoltre, invia automaticamente degli SMS ai cittadini che hanno frequentato gli stessi luoghi negli stessi giorni della persona infetta, segnalando gli spostamenti di quest'ultima. La Corea del Sud oltre a procedere ad una mappatura completa dei casi, diffondendo le generalità dei soggetti risultati positivi, quali età, sesso, indirizzo di casa e luogo di lavoro, ha sviluppato anche un'applicazione,

[49] I *Big Data* sono definiti come una «raccolta, analisi e accumulo di ingenti quantità di dati, tra i quali possono essere ricompresi dati di natura personale» (*Indagine conoscitiva sui Big Data*, realizzata dall'Autorità per le garanzie delle comunicazioni, l'Autorità garante della concorrenza e del mercato e il Garante per la protezione dei dati personali, 10 febbraio 2020, p. 7). Per un approfondimento si veda A. NICITA, M. DEL MASTRO, *Big Data. Come stanno cambiando il nostro mondo*, il Mulino, 2019.

[50] F.P. MICOZZI, *Le tecnologie, la protezione dei dati e l'emergenza coronavirus: rapporto tra il possibile e il legalmente consentito*, in *Biolaw Journal Instant Forum - Diritto, diritti ed emergenza ai tempi del Coronavirus*, 15 marzo 2020, p. 2. Si veda anche la riflessione *Il senso di Diritti Comparati per la crisi: emergenza, protezione dei diritti fondamentali e radici europee*, in *Dirittocomparati.it*, 1° aprile 2020.

[51] La sindrome respiratoria medio orientale (MERS-CoV) è una malattia infettiva che ha colpito molti stati dell'Asia già dal 2013.

[52] Il progetto "*smart city*" ha coinvolto il Ministero dell'Interno e della Sicurezza, il Ministero della Scienza, il Ministero delle Telecomunicazioni e il Ministero delle Infrastrutture e dei Trasporti, cfr. *South Korea Conceptualizes the Ultimate Smart City,* in *newcities.org.*

[53] *ncov.mohw.go.kr.*

ISSN 2279-7238

chiamata "*Corona100m*"[54]. L'*app*, dopo che l'interessato abbia prestato il consenso, registra le informazioni e la geolocalizzazione dello stesso, mostrandoli in via anonima e in tempo reale, rendendoli immediatamente disponibili a tutti gli iscritti. In ultimo, l'utente risponderà a delle domande sul proprio stato di salute che verranno condivise con le autorità preposte, le quali possono imporre, se necessario, la quarantena. I soggetti sottoposti a questa misura sono controllati da un funzionario governativo, che verifica le eventuali violazioni, attraverso accertamenti telefonici oppure con la geolocalizzazione.

Dall'analisi di tale sistema, è evidente che questa attività di *"contact tracing"* assicura un costante controllo sulla posizione e sullo stato delle persone risultate positive. L'utilizzo della tecnologia e di tutti i dati raccolti permette di ottenere grandi risultati: conoscere con esattezza i luoghi visitati dal soggetto infetto, isolare con una certa precisione le persone con cui sia venuto a contatto, individuare facilmente tutti i soggetti potenzialmente positivi[55]. È evidente, però, anche una forte compressione del diritto alla *privacy*, in nome della tutela alla salute. L'ordinamento sudcoreano, infatti, nonostante riconosca la riservatezza come un diritto costituzionalmente garantito[56], ha deciso di limitarlo fortemente per fronteggiare la situazione di emergenza. La Corea del Sud, dunque, ha preferito sacrificare completamente il diritto alla riservatezza, derogando al "*General Data Protection Regulation of South Korean*"[57] e, in particolare, al principio di minimizzazione dei dati, il quale stabilisce che il trattamento dei dati personali deve essere adeguato, pertinente e limitato a quanto necessario in relazione alle finalità che si vogliono perseguire[58].

L'utilizzo del dato personale, attraverso sistemi tecnologici, in una situazione di emergenza, certamente può assicurare maggiori forme di tutela, tuttavia, operare un giusto bilanciamento significa proteggere i diritti e gli interessi di tutti i cittadini, garantendo la dignità e il valore di ciascuno di essi, senza incidere totalmente sulla tenuta delle garanzie minime che uno Stato democratico deve mantenere.

Un altro paese che per far fronte alla pandemia ha deciso di voler utilizzare i sistemi tecnologici di sorveglianza, sacrificando il diritto alla *privacy*, è Israele.

La *Knesset* ha autorizzato la raccolta di dati personali dei cittadini da parte dell'agenzia di *intelligence* interna, lo *Shin Bet*, per combattere l'epidemia Covid-19[59]. Si assiste, dunque, ad un altro caso in cui viene consentita la possibilità di estrarre informazioni da telefoni cellulari privati per facilitare la gestione dell'emergenza da parte delle autorità. Lo *Shin Bet* può utilizzare a questo scopo gli strumenti solitamente impiegati per contrastare il terrorismo, anche se con maggiori restrizioni rispetto alle autorità giudiziarie[60].

---

[54] L'applicazione è scaricabile dal sito *mois.go.kr*.

[55] Le autorità coreane ritengono che tale sistema sia l'unico sistema per impedire la diffusione del virus, senza nel contempo azzerare le attività di un'intera nazione. Infatti, sono state implementate diverse applicazioni: *Corona100m, Coronamap e Coronaita*. Queste consentono di ricevere informazione sugli spostamenti dei contagiati, segnalando a quanti metri sono vicini.

[56] Constitution of the Republic of Korea, artt. 17 («*The privacy of no citizen shall be infringed*») e 18 («*The privacy of correspondence of no citizen shall be infringed*»).

[57] *Guidance on General data protection regulation of South Korean*, n. 4/2017.

[58] *Guidance on General data protection regulation of South Korean*, n. 4/2017, art. 5 (*Principles of personal data processing*).

[59] Agenzia di intelligence per gli affari interni di Israele.

[60] Le nuove norme emergenziali hanno autorizzato lo *Shin Bet* ad utilizzare il database segreto di intelligence, in cui vengono costantemente raccolte informazioni su ogni cittadino, per tracciare i pazienti affetti da coronavirus. La commissione Affari esteri e Difesa della Knesset ha dichiarato che la stessa ha approvato la decisione, consentendo allo «*Shin Bet di contribuire all'arresto della diffusione del coronavirus per un mese*» fino al 30 aprile *(knesset.gov.il)*. Tuttavia, non è scontato che le informazioni raccolte dallo *Shin Bet* non possano consentire ai positivi al coronavirus di essere

ISSN 2279-7238

Anche questo uso dei dati mostra una palese violazione della *privacy,* giustificata dal tentativo di fermare la diffusione del virus e inoltre, il fatto che la geolocalizzazione dei dispositivi mobili venga effettuata attraverso strumenti di *intelligence* antiterrorismo, suggerisce che al termine dell'emergenza sarà difficile tornare allo *status-quo ante*[61].

Infine, uno degli stati che fa della tecnologia il suo punto di forza per contrastare l'epidemia è la Cina. Il Presidente della Repubblica Popolare Cinese, Xi Jinping, avrebbe lanciato un appello[62] ai colossi dell'industria *tech* del Paese, quali *Alibaba, Baidu e Tencent*[63] per mettere a disposizione del governo le migliori innovazioni. Grazie ad applicazioni che utilizzano i *Big Data*, Intelligenza Artificiale, robotica e *device* connessi, l'esecutivo ha intensificato il suo sofisticato sistema di sorveglianza, che vanta circa 200 milioni di telecamere di sicurezza installate in tutto il Paese, per far rispettare la quarantena ai pazienti infetti e per mappare i movimenti del virus. Le autorità hanno così implementato un'*app*, chiamata *Alipay Health Code,* la quale assegna ad ogni cittadino un colore[64]. In base a questo, si decide chi può essere ammesso negli spazi pubblici, chi ha problemi di salute e chi deve restare a casa. L'*app* utilizza i *Big Data* in possesso dalla sanità cinese per identificare potenziali portatori del virus ed è stata adottata in oltre 200 città. Il maggior operatore telefonico del Paese, *China Mobile*, ha condiviso con alcuni *media* i dati di spostamento dei suoi utenti affetti da virus al fine di tracciare, in determinate città, le possibilità di contagio. L'efficienza della macchina tecnologica cinese, però, seppur giustificata da una cultura di fondo, sociale e giuridica molto distante dalla nostra, viola palesemente la riservatezza dei dati. Tutti i *device* sin ora menzionati, infatti, richiedono agli utenti di registrarsi con il loro nome, numero di identificazione nazionale e numero di telefono, incidendo su possibili casi di discriminazione verso i cittadini risultati positivi al coronavirus (si pensi alla "caccia all'untore") o di eccessiva invasione dei propri dati personali. Ad esempio, attraverso una ricerca *online* sul codice della segnalazione si possono recuperare ulteriori dettagli della persona contagiata, tra i quali, volto, fotografie o anche elementi relativi ai familiari. Il sistema di analisi automatizzata dei dati incrociati, dunque, pur consentendo, mediante l'ausilio di algoritmi di Intelligenza Artificiale, di intervenire con azioni di prevenzione e contenimento più rapide e mirate, non può essere trapiantato nel nostro Paese. Le nostre azioni devono ispirarsi alla Costituzione e non al "governo dell'emozione"[65].

---

inconsapevolmente identificati tramite la loro attività telefonica, una volta terminata l'emergenza. Sul tema si veda, S. ELDAR, *Coronavirus crisis exposis Shin Bet's secret database*, in *al-monitor.com*, 1°aprile 2020.

[61]Alcune associazioni per i diritti civili e la tutela delle minoranze in Israele hanno immediatamente segnalato le loro preoccupazioni, affermando che strumenti così invasivi per la lotta contro il coronavirus e la necessità di sorvegliare i contagiati calpestano i diritti individuali e le norme democratiche. Cfr., *Ibidem.* Il tema della tendenza espansiva delle discipline speciali ed emergenziali è centrale in un ordinamento democratico. Anche nel nostro ordinamento si è discusso del tema con riferimento alla legislazione anti Brigate Rosse, applicata poi anche al fenomeno mafioso, fino ad arrivare alla lotta al terrorismo. Pe runa riflessione, si veda A. BLANDO, *La normale eccezionalità. La mafia, il banditismo, il terrorismo e ancora la mafia*, in *Meridiana*, 2016, pp. 173-202.

[62] B. SIMONETTA, *Così big data e intelligenza artificiale stanno battendo il coronavirus in Cina*, 9 marzo 2020, in *ilsole24ore.com.*

[63] *Alibaba Group* è una multinazionale cinese privata con sede ad Hangzhou composta da una serie di società attive nel campo del commercio elettronico, quali mercato online, piattaforme di pagamento e compravendita, motori di ricerca per lo shopping e servizi per il *cloud computing. Baidu* è il principale motore di ricerca in lingua cinese in grado di ricercare siti web, file audio e immagini. *Tencent Holdings Limited* è una società per azioni d'investimento fondata nel 1998 che fornisce servizi in materia di intelligenza artificiale, internet e prodotti tecnologici.

[64]Il sistema assegna automaticamente alle persone uno dei tre codici colore (verde, giallo o rosso) in base alla loro cronologia di viaggio, il tempo trascorso negli *hotspot* dell'epidemia e l'esposizione a potenziali portatori del virus. Questo per decidere chi deve mettersi in quarantena o se possano spostarsi liberamente. G. ZUNINO, *Coronavirus, app e sistemi per tracciare i positivi: come funzionano (nel mondo, in Italia), in Agendadigitale.ue, 23.04.2020.*

[65] Come affermato anche da Antonello Soro nell'intervista "*In uno stato d'eccezione è lecito rinunciare a qualche libertà. Ma il nostro modello non potrà mai essere la Cina*", pubblicata il 19 marzo 2020 in *garanteprivacy.it.*

ISSN 2279-7238

Infatti, appare ragionevole la ricerca di soluzioni tecnologiche che si affianchino alle misure di prevenzione, diagnosi e cura adottate sino ad ora[66], purché siano orientate verso criteri di gradualità, con la possibilità di valutare se misure meno invasive possano essere sufficienti a fini di prevenzione. Ad esempio, apparirebbe sproporzionato sia richiedere (e poi trattare a fini statistici) l'età, il sesso o il datore di lavoro durante la fase di registrazione ad un'applicazione, sia geolocalizzare tutti i cittadini, 24 ore su 24, nel caso in cui esista già una misura di distanziamento sociale, non soltanto per l'invasività della misura, ma anche perché la gigantesca mole di dati così acquisita non avrebbe una effettiva utilità nella lotta alla diffusione. L'emergenza, dunque, deve poter considerare ogni deroga possibile purché non irreversibile; non dev'essere, in altri termini, un punto di non ritorno ma un momento in cui modulare prudentemente il rapporto tra norma ed eccezione[67].

4. Conclusioni: l'innovazione tecnologica e i limiti invalicabili dello Stato di diritto

Alla luce della ricognizione interna e comparata sin ora svolta, è possibile una riflessione di più ampio respiro sulle modalità di utilizzo dei dati personali per fronteggiare l'epidemia. La nostra società è come un Giano Bifronte: da una parte guarda verso il futuro e ad una sempre maggiore tecnologizzazione; mentre dall'altra è ancora legata a riflessioni sviluppatesi nei secoli scorsi sulla scorta del pensiero liberale, primo tra tutti la diffidenza verso uno Stato poliziesco [68] o "controllore". Si avvicinano a quest'ultimo modello gli strumenti adottati dagli stati analizzati nel paragrafo precedente, che come abbiamo visto non sono compatibili in un contesto liberal-democratico come il nostro. Il governo italiano, infatti, ha cercato di non spingersi oltre i limiti implicitamente invalicabili di uno Stato di diritto: è consapevole che l'utilizzo di dati personali e di *device* tecnologici, in una situazione di crisi, possa essere idoneo al contenimento dell'emergenza, ma che tale scelta debba essere sempre la meno invasiva della sfera personalissima dei cittadini. Il trattamento dei dati a fini statistici e l'aggregazione di questi per ricavare le informazioni desiderate denotano l'importanza ormai imprescindibile degli stessi, anche sotto il valore economico[69]. I sistemi cinesi, sudcoreani e israeliani hanno ottenuto dei risultati notevoli sul piano della mappatura dell'emergenza, con il vantaggio di contenere il virus senza dover arrestare il sistema produttivo di un Paese, sacrificando, però, il diritto alla riservatezza. Infatti, avendo avuto accesso ad una quantità notevole di dati, probabilmente eccessiva, esiste anche il timore che le misure adottate in tali periodi di emergenza diventino poi "permanenti"[70].

---

[66] M. PROVERBIO, *Bilanciare privacy, economia e salute,* in *ilSole24ore*, 5 aprile 2020, p.13.

[67] Come sottolineato da Antonello Soro nell'intervista "*Privacy e democrazia ai tempi della pandemia*", pubblicata il 24 marzo 2020, in *garanteprivacy.it*.

[68] Si accoglie in questa sede la differenza tra Stato di polizia e Stato poliziesco presente in F. MODUGNO, *Ordinamento – Diritto – Stato*, in IDEM (a cura di), *Diritto Pubblico*, Giappichelli, 2019, pp. 73-74.

[69] È stato osservato che la disponibilità di informazioni sui comportamenti e sulle preferenze degli individui, estratte mediante l'analisi dei *Big Data*, ha reso possibile un cambio di paradigma nel processo decisionale delle imprese. Quest'ultime riescono ad evitare analisi preliminari di mercato relative al prodotto da offrire, grazie ai dati detenuti e alle correlazioni tra gli stessi. Infatti, il valore di questi non risiede nella loro disponibilità, quanto nella loro qualità, cfr. *Indagine conoscitiva sui Big Data*, cit., p. 18.

[70] Y. N. HARARI, *The world after coronavirus*, in *ft.com*, 20 marzo 2020.

ISSN 2279-7238

L'Italia, oramai, sull'esempio della Corea del Sud[71], si sta muovendo verso l'innovazione tecnologica come strumento di lotta alla diffusione della pandemia. Ad esempio, si pensi all'*app* AllertaLOM[72] o all'*app* Immuni[73], istituita presso il Ministero della Salute. Quest'ultima, in particolare, è la piattaforma che verrà utilizzata per il tracciamento di contagi (l'effettivo funzionamento è stimato per la fine del mese di maggio), al solo fine «*di rintracciare le persone che siano entrate in contatto con soggetti risultati positivi e tutelarne la salute attraverso le previste misure di profilassi nell'ambito delle misure di sanità pubblica legate all'emergenza Covid-19*»[74]. Il trattamento effettuato per il tracciamento dei contatti è basato sul trattamento di dati di prossimità dei dispositivi, resi anonimi oppure, dove non sia possibile, pseudoanonimizzati. Inoltre, è su base volontaria, realizzata esclusivamente con «*infrastrutture localizzate sul territorio nazionale e gestite da amministrazioni o enti pubblici o in controllo pubblico*»[75] e il mancato utilizzo dell'applicazione non comporta alcuna limitazione o conseguenza in ordine all'esercizio dei diritti fondamentali dei soggetti interessati.

L'obiettivo, infatti, è quello di utilizzare solo i dati personali degli utenti che si serviranno dell'*app*, che saranno individuati secondo criteri stabiliti dal ministero della Salute, per avvisarli nel

---

[71] Riprodurre il modello sud-coreano significherebbe limitare fortemente il diritto alla riservatezza, ma avrebbe il pregio di tutelare pienamente il diritto alla salute e di consentire il funzionamento dell'economia del Paese. La sfida, dunque, potrebbe essere quella di non rifiutare a priori tale filosofia di intervento, ma attuandola studiando con quali garanzie e soluzioni operative si possa renderla compatibile compatibilità con il diritto alla *privacy*.

[72]Altre regioni hanno sviluppato proprie applicazioni per contenere il contagio, ad esempio la Campania, prima del Decreto-legge 30 aprile 2020, n. 28, avrebbe deciso di mappare i soggetti in forma anonima senza associare i dati degli spostamenti ad un nominativo. È stato infatti necessario contenere le diverse iniziative regionali e garantire una disciplina uniforme a livello nazionale. Per un approfondimento, si veda l'intervista di V. DI GIACOMO ad Antonello Soro, *Le app degli spostamenti solo su base volontaria*, in *Il Mattino*, 17 aprile 2020, p. 5.

[73]Il Ministro per l'Innovazione tecnologica e la digitalizzazione, di concerto con il Ministero della Salute, l'Istituto Superiore di Sanità (Iss) e l'Organizzazione Mondiale della Sanità (Oms), ha rivolto un invito al mondo dell'impresa e della ricerca. La *call* si sviluppa all'interno dell'iniziativa "*Innova per l'Italia*" ed ha avuto come obiettivo quello di individuare le migliori soluzioni digitali disponibili relativamente ad *app* di telemedicina e assistenza domiciliare dei pazienti e a tecnologie e strategie basate sulle tecnologie per il monitoraggio "attivo" del rischio di contagio, e coordinare a livello nazionale l'adozione e l'utilizzo di queste soluzioni e tecnologie, al fine di migliorare i risultati in termini di monitoraggio e contrasto alla diffusione del Covid-19.

In data 8 aprile, infatti, il ministro Pisano ha svolto un'audizione informale davanti la Commissione IX (Trasporti, Poste e Telecomunicazioni) della Camera dei Deputati. In questa sede ha riassunto le linee guida della "*app*", oggetto di studio da parte del gruppo di esperti *ex* art. 76, comma, 1, d.l. 18/2020. Il Ministro ha anche chiarito «*che raggiunta la finalità perseguita, tutti i dati ovunque e in qualunque forma conservati, con l'eccezione di dati aggregati e pienamente anonimi a fini di ricerca o statistici, saranno cancellati con conseguente garanzia assoluta per tutti i cittadini di ritrovarsi, dinanzi a soggetti pubblici e privati, nella medesima condizione nella quale si trovavano in epoca anteriore all'utilizzo della* app *di* contact tracing» Per il titolare del dicastero dell'Innovazione tecnologica «*si tratta di un terreno delicato, ed è indispensabile, a tal fine, che il singolo possa confidare nella trasparenza e nella correttezza delle caratteristiche del servizio nonché nell'assenza del perseguimento di scopi ulteriori e incompatibili con la finalità di prevenzione sanitaria*» (i virgolettati sono tratti da M. PENNISI, *Coronavirus, spinta dell'Europa per l'app «unica». Task force italiana vicina alla scelta*, in *Corriere.it*, 8 aprile 2019).

Anche la Commissione europea sta lavorando ad un'*app* di tracciamento ed aveva individuato la data del 15 aprile come termine per l'elaborazione di un «*pacchetto di strumenti per un approccio paneuropeo per le applicazioni mobili*» da parte degli Stati membri in collaborazione con il comitato europeo per la protezione dei dati (M. PENNISI, *Coronavirus, spinta dell'Europa per l'app «unica». Task force italiana vicina alla scelta*, Corriere.it, 9 aprile 2020; si veda anche *Lettera della Presidente del Comitato Europeo per la Protezione dei Dati alla Commissione europea sul Progetto di linee-guida in materia di app per il contrasto della pandemia dovuta al Covid-19*, 15 aprile 2020; *Commissione Ue su app per tracciamento. Dichiarazione di Antonello Soro, Presidente dell'Autorità garante per la privacy*, in *garanteprivacy.it*, 16).

[74]Decreto-legge 30 aprile 2020, n. 28 Misure urgenti per la funzionalità dei sistemi di intercettazioni di conversazioni e comunicazioni, ulteriori misure urgenti in materia di ordinamento penitenziario, nonché disposizioni integrative e di coordinamento in materia di giustizia civile, amministrativa e contabile e misure urgenti per l'introduzione del sistema di allerta Covid-19.

[75]Decreto-legge 30 aprile 2020, n. 28 Misure urgenti per la funzionalità dei sistemi di intercettazioni di conversazioni e comunicazioni, ulteriori misure urgenti in materia di ordinamento penitenziario, nonché disposizioni integrative e di coordinamento in materia di giustizia civile, amministrativa e contabile e misure urgenti per l'introduzione del sistema di allerta Covid-19.

ISSN 2279-7238

caso abbiano avuto stretti contatti con altri utenti accertati positivi al virus, in modo da agevolare l'eventuale adozione di misure di assistenza sanitaria in favore degli stessi soggetti. In ultimo, come già detto, è previsto un termine entro il quale dovrà essere interrotto ogni trattamento di dati personali: secondo il decreto-legge n. 28, la data di cessazione dovrebbe coincidere con la fine dello stato di emergenza e comunque non oltre il 31 dicembre 2020.

Queste proposte, attentamente monitorate anche dal Garante privacy [76], sembrerebbero rispettare il principio di proporzionalità di cui sopra, ma sarà importante che nei prossimi sviluppi non si tenda ad imitare pedissequamente i modelli eccessivamente lesivi della riservatezza.

Nella situazione che stiamo vivendo, la Protezione civile e le altre autorità delegate possono sfruttare i dati sensibili anche per ricerche a fini statistici-scientifici o per ottimizzare trattamenti sanitari, ma i dati devono rimanere in possesso solo di questi. Infatti, solo tali soggetti dovrebbero informare le persone che sono entrate in contatto con chi è risultato positivo al virus o si sospetta che lo abbia, ma senza fornire le generalità, in modo da tutelare il diritto alla *privacy*. Inoltre, anche la strada dell'anonimizzazione deve essere percorsa con cautela, in quanto si sono evidenziati i rischi di re-identificazione degli interessati utilizzando *dataset* ulteriori (pur privi di identificativi individuali)[77].

Si auspica, dunque, che il Governo, in tale situazione emergenziale, continui verso questa direzione, comprendendo l'utilità di porre in correlazione sistema sanitario, forze dell'ordine e istituzioni attraverso la tecnologia, ma restando nei binari delle garanzie costituzionali[78]. Infatti, affidarsi esclusivamente a commissioni e criteri meramente tecnici condannerebbe il diritto ad un ruolo ancillare rispetto alla tecnica[79].

[76] A. SORO, Parere sulla proposta normativa per la previsione di una applicazione volta al tracciamento dei contagi da Covid-19, in *garanteprivacy.it, 29 aprile 2020;* A. SORO, *Audizione informale, in videoconferenza, del Presidente del Garante per la protezione dei dati personali sull'uso delle nuove tecnologie e della rete per contrastare l'emergenza epidemiologica da Coronavirus*, in *garanteprivacy.it*, 8 aprile 2020.

[77] Per un approfondimento sul tema, si veda *Indagine conoscitiva sui Big Data*, realizzata dall'Autorità per le garanzie delle comunicazioni, l'Autorità garante della concorrenza e del mercato e il Garante per la protezione dei dati personali, 10 febbraio 2020, p. 61.

[78] Sul punto, G. AZZARITI, *Editoriale. Il diritto costituzionale d'eccezione*, in *Costituzionalismo.it*, n, 1/2020, pp. 2-3; B. CARAVITA DI TORITTO, *L'Italia ai tempi del coronavirus: rileggendo la Costituzione italiana*, in *Federalismi.it,* n. 6/2020; T. GROPPI, *Le sfide del coronavirus alla democrazia costituzionale*, in *Consulta-Online*, n. 1/2020.

[79] Per un maggior approfondimento, si veda A. FARANO, *La Repubblica degli scienziati? Saperi esperti e biopolitica ai tempi del coronavirus,* in *Biolaw Journal Instant Forum - Diritto, diritti ed emergenza ai tempi del Coronavirus*, 28 marzo 2020.

ISSN 2279-7238

ABSTRACT

Il contributo analizza la normativa italiana in materia di tutela dei dati personali e le eccezioni al GDPR, che si sono rese necessarie durante l'emergenza Covid-19. Bisogna chiedersi, infatti, se uno stato democratico possa sacrificare indistintamente alcuni diritti a favore di quello alla salute, anche attraverso l'uso della tecnologia. Inoltre, il diritto alla protezione dei dati personali muta a seconda del contesto democratico, culturale e giuridico di un ordinamento e per questi motivi si sono volute analizzare anche le risposte all'emergenza da parte di tre sistemi non europei, in cui il concetto di diritti è molto diverso: Corea del Sud, Israele e Cina.

The contribution aims to summarily analyze the rules in the field of personal data and the exceptions to the GDPR, due to the Covid-19 emergency. Italy, during this emergency, in order to avoid a tyranny by law to health, tries to find suitable means to protect the right to privacy.
In this situation, it is necessary to ask how a democratic state can sacrifice some rights to carry out a strategy, also through the use of technology and personal data, and how much the right to the protection of personal data can be subject to a different discipline based on the democratic, cultural and legal context. For these reasons, it was necessary analyze also three non-European systems, where the concept of rights is very different: South Korea, Israel and China.

PAROLE CHIAVE: Covid-19 – protezione dei dati personali – GDPR – diritto alla salute – geolocalizzazione;

KEYWORDS: Covid-19 – *protection of personal data* – GDPR – right to health – geolocation;

ISSN 2279-7238