OPINIO JURIS
LAW & POLITICS REVIEW

Diritto alla privacy nell'attuale contesto emergenziale: cedevolezza della tutela e normalizzazione della sorveglianza?

Come e quando nasce il diritto alla "privacy"? perché è tutelato? I dubbi legati al "contact tracing" e i nuovi modelli di gestione.

Di

Antonio Fabio Vigneri

«Salus populi suprema lex esto»
Cicerone, *De Legibus*

I. Introduzione: le nuove sfide del costituzionalismo

«Il potere dello Stato è fatalmente destinato a restare sempre un male pericoloso, anche se necessario […]. *Il prezzo della libertà è l'eterna vigilanza»*: così ammonisce l'epistemologo Karl Popper ne "*La società aperta e i suoi*

ISSN 2531-6931

nemici"[1] (1945), opera destinata nell'attuale contesto di emergenza, di conflittualità diffusa e di imprevedibilità nelle relazioni internazionali a una necessaria rilettura.

Al giorno d'oggi la vigilanza è sempre più complessa e impegnativa in quanto le democrazie occidentali si trovano ad affrontare particolari minacce insidiose: la permanente criminalità organizzata transazionale; il rischio nucleare; la minaccia bellica, sebbene attenuata; il pericolo cibernetico; il terrorismo di matrice islamico-radicale e il rischio epidemiologico, che da fenomeno locale ha assunto i connotati di una minaccia globale. Tutto ciò richiede l'impiego di risorse umane e tecnologiche qualitativamente commisurate alla gravità dei rischi.

Proprio tale ultima forma di minaccia, manifestatasi con la diffusione del coronavirus 2019-nCoV (meglio noto come COVID-19), a partire da un mercato di Wuhan specializzato nella vendita di animali vivi, ha comportato l'adozione di misure eccezionali, ponendo il problema della compatibilità di dette misure, poste a presidio della collettività, con i diritti fondamentali riconosciuti dalla Costituzione repubblicana. Trattasi di misure eccezionali attuate mediante una copiosa produzione normativa, necessaria conseguenza della dichiarazione dello stato di emergenza proclamato con la Delibera del Consiglio dei Ministri del 31 gennaio 2020 (*"Dichiarazione dello stato di emergenza in conseguenza del rischio sanitario connesso all'insorgenza di patologie derivanti da agenti virali trasmissibili"*).

Le misure di contenimento implementate dall'Esecutivo italiano hanno proiettato la collettività nella più vasta e massiccia esperienza di limitazione dei diritti costituzionali mai avvenuta nella storia d'Italia. Un corposo novero di diritti e libertà fondamentali è stato, pertanto, sottoposto a severe restrizioni: si pensi alla libertà personale e di circolazione, alla libertà religiosa e al diritto all'educazione, alla

[1] *La società aperta e i suoi nemici. Platone totalitario - vol. I*, K. R. POPPER, D. ANTISERI (a cura di), Armando, Roma, 2014, pp. 11-632.

protezione dei dati personali e alla *privacy*, alle libertà associative, alla libertà economica e ai diritti dei lavoratori.

Fatta questa necessaria premessa, il presente lavoro si soffermerà, in particolare, sulla valutazione delle limitazioni apportate alla protezione della *privacy* e dei dati personali. Molto dibattuto, nel momento in cui si scrive, è, infatti, il tema delle possibili limitazioni del diritto alla *privacy* determinate dal tracciamento degli spostamenti collettivi, finalizzato a riannodare la catena di contagio del virus e, conseguentemente, a poter apprestare una reazione più efficace e mirata. Occorrerà necessariamente domandarsi fino a che punto tali attività di *contact tracing* possano spingersi.

§II. **Invenzione, reinvenzione e fine della *privacy***

Il diritto alla *privacy* cominciò a delinearsi intorno al XIX secolo, sebbene una tale esigenza di protezione abbia
ragioni molto più antiche: si pensi all'importanza per il mondo greco della distinzione tra spazio pubblico (*polis*) e dimensione privata (*oikos*). Peraltro, nel mondo antico, l'idea di *privacy* era di regola riferita non tanto alla persona in sé ma allo stesso spazio domestico. La sua percezione veniva, pertanto, ricondotta e intrecciata ad altre sfere di tutela[2]. Nonostante le radici antiche, un autonomo diritto alla *privacy* della persona ha stentato ad affermarsi, riconoscendosi in esso soltanto una componente di altri diritti, primariamente del diritto di proprietà. Inoltre, il diritto *de quo* è stato riconosciuto e tutelato *in primis* nei Paesi di *common law* e, solo in un secondo momento, in quelli di *civil law*.
Anzitutto analizziamo l'origine del termine e la definizione.

Si tratta di un concetto terminologicamente e sostanzialmente di importazione anglosassone, il cui atto di nascita, come nozione giuridica, può rinvenirsi in un ormai celebre articolo pubblicato presso

[2] *Le indagini penali. Profili strutturali di una metamorfosi investigativa*, S. SIGNORATO, Giappichelli, Torino, 2018, p. 72.

ISSN 2531-6931

la prestigiosa *Harvard Law Review*, ad opera dei due giuristi bostoniani Samuel D. Warren e Louis D. Brandeis.

"*The Right to Privacy*"[3], ritenuto uno dei saggi più influenti nella storia del diritto americano e ampiamente considerato la prima pubblicazione negli Stati Uniti a disciplinare il diritto alla *privacy*, ne indica efficacemente il nucleo nel c.d. *right to be let alone*: il diritto a essere lasciati soli.

La teorizzazione del diritto alla *privacy* avvenne nel contesto di una diffusione di notizie a mezzo stampa, volte non a informare, ma a creare scandalo. Warren, infatti, era stato oggetto di vari pettegolezzi divulgati dalla stampa scandalistica della città. Precisamente, la gazzetta locale diede largo risalto, nelle cronache mondane, a degli eventi di lusso, organizzati dallo stesso Warren. Tale giornale criticava l'ostentazione finanziaria di Warren, facendo anche considerazioni poco benevole sullo spreco di denaro. Warren si associò all'avvocato Brandeis; scrissero l'articolo e avviarono un'azione legale per protestare contro l'invadenza della stampa e per invocare il rispetto della sua vita privata. Questa veniva intesa, peraltro, non in senso strettamente individuale, ma in quello familiare. In altre parole, i due avvocati intervennero per tutelare le persone da ogni indebita intrusione nella loro vita privata. Anni dopo la Corte Suprema riconobbe il *right to privacy* che divenne una pietra miliare del diritto costituzionale americano [4] . Tale garanzia, sebbene prevista nell'ordinamento americano ha, tuttavia, faticato non poco a essere accolta nella legislazione europea, più orientata a soluzioni individuali che generali.

Quanto agli aspetti definitori, è stato rilevato che il termine *privacy «indica due concetti affini e parzialmente sovrapponibili, quello di riservatezza e*

[3] *The Right to Privacy*, S. WARREN, L. D. BRANDEIS, in *Harward Law Review*, 5, 1890, p. 4 e ss.
[4] *Privacy: diritto fondamentale oppure no*, FROSINI T. F., in *Federalismi*, n. 16/2008, p. 1, https://www.federalismi.it/ApplOpenFilePDF.cfm?artid=10767&dpath=document&dfile=06082008154616.pdf&content=Privacy%3A%2Bdiritto%2Bfondamentale%2Boppure%2Bno%2B%2D%2Bstato%2B%2D%2Bdottrina%2B%2D%2B, ultimo accesso il 7 maggio 2020.

quello di privatezza. Il termine, inizialmente utilizzato per indicare l'inviolabilità della soglia domestica, nell'era digitale indica il controllo sulle informazioni che ci riguardano ed è l'ultima barriera alla bulimia della sorveglianza elettronica»[5]. La tutela della *privacy* è stata, in un primo momento, interpretata in senso passivo, per erigere un confine invalicabile a tutela del singolo e della sua famiglia e, in un secondo momento, in senso attivo, relativamente alla libertà di compiere scelte personali in completa sicurezza e autonomia[6].

Il vocabolo in esame – che spesso viene utilizzato come sinonimo di "riservatezza", "vita privata", "intimità della vita privata" [7] – presenta un originario nucleo privativo, una iniziale valenza prevalentemente negativa, indicativa di un diritto volto a privare gli altri della conoscenza di sé. Si tratta, dunque, un diritto a non subire illegittime interferenze altrui nella propria sfera individuale e, dunque, un *diritto ad essere lasciati soli.*

Progressivamente, il concetto di *privacy* si è ampliato, tanto che autorevole dottrina[8] ha rinvenuto nel termine *de quo* una "costellazione di diritti". Tale concetto ha gradatamente iniziato a ricomprendere, inoltre, il diritto di potere esercitare un monitoraggio delle proprie informazioni sia nel momento della loro acquisizione, sia in momenti successivi. Un siffatto principio di c.d. "autogestione informativa", tuttavia, viene a scontrarsi con le pratiche autoritarie di gestione del potere di taluni Stati – quali Cina, Iran, Vietnam, Russia, Arabia Saudita, etc. – in cui le attività di *censorship* limitano o vietano la circolazione delle informazioni.

Il diritto alla riservatezza, nato e costruito nella prevalente dimensione socio-relazionale[9], da una sfera intima e privata ha assunto

---

[5] *Un dizionario hacker*, A. DI CORINTO, Manni, San Cesario di Lecce, 2014, p. 168.
[6] *Ivi*, pp. 169-170.
[7] Come messo in evidenza da P. PATRONO, voce *Privacy e vita privata (dir. pen.)*, in *Enc. Dir.*, vol. XXXV, Milano, 1986, p. 559.
[8] *I nuovi diritti nella giurisprudenza costituzionale*, F. MODUGNO, Giappichelli, Torino, 1995, p. 20.
[9] *Brevi riflessioni su privacy e costituzionalismo al tempo dei big data*, L. CALIFANO, in *Federalismi*, n. 3/2017, p. 3, https://www.federalismi.it/ApplOpenFilePDF.cfm?eid=438&dpath=editoriale&dfile=EDITORIALE%5F02052017161209%2Epdf&content=Brevi%2Briflessioni%2Bsu%2Bprivacy%2Be%2B

ISSN 2531-6931

nel tempo il connotato di un diritto a mantenere il controllo sulle proprie informazioni e di determinare le modalità di costruzione della propria immagine senza manipolazioni e distorsioni indebite.

Nell'attuale "età dei diritti", teorizzata da Bobbio[10], non si parla più di "Stato di diritto" bensì di "Stato dei diritti", facendosi riferimento all'istituzione di uno "spazio dei diritti", che individua un connotato essenziale nello Stato costituzionale. Tale dimensione dei diritti deve, tuttavia, adeguarsi alla società dell'informazione e alla fisionomia del *cyberspace*, caratterizzato per la cancellazione dei vincoli di tempo e di spazio[11]. In un contesto siffatto cambia il concetto di identità e di *privacy*.

Il *social networking*, emblema del Web 2.0, esprime in modo radicale questo mutamento di prospettiva. Nell'ecosistema delle cc.dd. "reti sociali", si rendono note all'esterno un insieme di informazioni personali, quello che Rodotà chiama "corpo elettronico"[12]. Si invoca, così, una *«libertà da vincoli irragionevoli alla costruzione della propria identità»*[13]. Nella società dell'informazione, ormai migrata verso l'esibizione dell'io più intimo, la "cooperazione della vittima", unita alle risorse e ai poteri di controllo statali, abbassa notevolmente il margine di difesa dell'individuo.

costituzionalismo%2Bal%2Btempo%2Bdei%2Bbig%2Bdata&content_auth=%3Cb%3ELicia%2BCalifano%3C%2Fb%3E, ultimo accesso il 7 maggio 2020.

[10] *L'età dei diritti*, N. BOBBIO, Einaudi, Torino, 1990.

[11] A questo proposito, autorevolmente, S. RODOTÀ, *Il diritto di avere diritti*, Laterza, Roma-Bari, 2012, p. 379, rileva che *«Internet, il più grande spazio pubblico che l'umanità abbia conosciuto, la rete che avvolge l'intero pianeta, non ha sovrano* […]. *Più Internet cresce(va), acquistando così una rilevanza sociale e politica sempre maggiore, più si è fatta aggressiva la pretesa degli Stati di far valere le loro antiche prerogative, di continuare a considerare la rete come l'oggetto del desiderio delle sovranità esistenti* […]. *Gli Stati nazionali cercano di far valere il potere, tutt'altro che residuale, di cui ancora dispongono, ma non possono stabilire una sovranità sul cyberspazio».* In ultima analisi, preso atto di una incoercibilità dello spazio cibernetico – continua l'Autore – può concludersi per una *«impossibilità, inutilità, illegittimità di qualsiasi regolazione di Internet».*

[12] *Ivi*, p. 322.

[13] *Technology and Privacy. The New Landscape*, P.E. AGREE e M. ROTEMBERG, Mit Press, Cambridge (Mass.) 2001, p. 7.

La tradizionale nozione di *privacy* – lo si è detto – inizialmente costruita come un dispositivo "escludente", muta profondamente nel contesto della c.d. *Information Age*[14]. La sua costruzione originaria, infatti, riproduce lo schema della proprietà privata, *ius excludendi omnes alios*, all'interno della quale nessuno può legittimamente penetrare. La rivoluzione dell'informazione, tuttavia, ha trasformato la nozione stessa di sfera privata che, notevolmente ridotta, è divenuta sempre più intensamente luogo di scambi, di condivisione di dati personali di informazioni la cui circolazione non riguarda più soltanto quelle in uscita, di cui gli altri possono appropriarsi o venire a conoscenza, ma interessa anche quelle in entrata, con le quali gli altri invadono la sfera individuale in forme sempre più massicce e indesiderate.

Si è potuto così affermare che l'*habeas corpus*, presidio dell'intangibilità della persona derivante dalla *Magna Charta Libertatum* del 1215[15], debba declinarsi seconda una nuova prospettiva. Dal rispetto del corpo "fisico" nella sua integralità, la dottrina[16] ne ha tratto il rispetto del corpo "elettronico". Secondo tale nuova lettura, la *data protection* adempie alla funzione di assicurare quell'"*habeas data*" che i tempi mutati esigono, diventando così, com'è avvenuto con l'*habeas corpus*, un elemento inscindibile dalla civiltà. Si afferma, in altre parole, un diritto a mantenere il controllo dei propri dati informatici personali, compresa la facoltà di impedirne la circolazione. A causa, di una costante produzione di dati che riguardano l'individuo, si trova,

[14] Per un'analisi dettagliata sull'ampio concetto di *Information Age* si rinvia a L. FLORIDI, *La rivoluzione dell'informazione*, Codice Edizioni, Torino, 2012. In tale opera l'Autore analizza l'ambiente nel quale si diffonde l'interazione tra individui e l'informazione, dimostrando come *«sotto molti profili non siamo entità isolate, quanto piuttosto organismi informazionali interconnessi, o inforg, che condividono con agenti biologici e artefatti ingegnerizzati un ambiente globale costituito in ultima analisi dalle informazioni, l'infosfera»*.

[15] La *Magna Charta Libertatum*, una delle pietre miliari del costituzionalismo, all'art. 39 stabiliva che *«Nessun uomo libero sarà arrestato, imprigionato, multato, messo fuori legge, esiliato o molestato in alcun modo, né noi useremo la forza nei suoi confronti o demanderemo di farlo ad altre persone, se non per giudizio legale dei suoi pari e per la legge del regno»*.

[16] *Privacy, libertà, dignità.* ***Discorso conclusivo della Conferenza internazionale sulla protezione dei dati***, S. RODOTÀ, Garante per la Protezione dei Dati Personali, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1049293, ultimo accesso il 6 maggio 2020.

ISSN 2531-6931

pertanto, a operare nella società con una sorta di "doppio corpo", quello fisico-naturale e quello elettronico-artificiale che costituisce una "seconda persona".

Senza una forte tutela del "corpo elettronico" si rafforzano le spinte verso una costruzione di una società della sorveglianza, della classificazione e della selezione sociale, basata su attività di *data mining* sempre più aggressive e capillari, motivate da esigenze di sicurezza o di mercato e consistenti nell'incessante ricerca di informazioni sui comportamenti di ciascuno e nell'estrapolazione di profili individuali, familiari e di gruppo. In un contesto che sempre più nettamente trasforma gli individui in "*networked persons*", persone perennemente in rete, via via configurate in modo da emettere e ricevere impulsi che consentono di rintracciare e ricostruire movimenti, abitudini, contatti, si modificano il senso e i contenuti dell'autonomia delle persone, e quindi si incide sulla loro dignità. La *privacy* diviene strumento necessario per salvaguardare la società della libertà e si configura come componente essenziale della c.d. "società della dignità"[17].

Quanto alla "fine della *privacy*" nell'odierna società dell'informazione, analizzata, inoltre, dal lato dell'utente, può farsi riferimento alla diffusione volontaria da parte dell'individuo di dati che lo riguardano e all'impossibilità successiva della rimozione degli stessi. Si assiste, infatti, a una difesa della *privacy* che appare rifiutata dai comportamenti sociali attraverso una mancanza di sensibilità nella protezione dei dati, comportante una sorta di "svendita" della *privacy* da parte del cittadino stesso ben disposto, poi, a invocarne la tutela solo quando venga sofferto un danno[18].

Accanto alla mancata percezione del valore della protezione dei dati si aggiunge il problema della mancata comprensione della persistenza degli stessi nelle Rete. Da qui si origina il dilemma del c.d. "diritto

[17] *Ibidem*.

[18] *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, G. ZICCARDI, Raffaello Cortina Editore, Milano, 2015, pp. 147-148-149.

all'oblio", il diritto a essere dimenticati che si realizza, in concreto, mediante la rimozione in forma rafforzata di tutti quei *link* e quei riferimenti che rimandano ad un contenuto *online* lesivo per il soggetto, per la sua immagine e per la sua vita di relazione, specie quando il contenuto eliminato attiene a condanne o a fatti che possono destare riprovazione sociale.

§III. **Ricognizione normativa e giurisprudenziale del diritto alla *privacy***

Preliminarmente, va rilevato che alla concezione statica del concetto di *privacy*, così come originariamente inteso, si è accostata – come conseguenza di un ampliamento della nozione stessa – una concezione per così dire dinamica, coincidente con il diritto all'autodeterminazione informativa e con il configurarsi del diritto alla protezione dei dati personali. Con l'ingresso nella società dell'informazione, la riservatezza viene definita come un diritto "multidimensionale", in grado di tenere conto adeguatamente di molteplici e differenti interessi[19].
Il diritto alla *privacy* trova un riscontro normativo in fonti sovranazionali e nazionali. Nella Carta dei diritti fondamenti dell'Unione europea si tiene conto della nuova visione dinamica del diritto in esame. Nella Carta di Nizza del 2000, avente lo stesso valore giuridico dei Trattati istitutivi, infatti, all'art. 8[20] il diritto alla protezione

[19] *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, S. NIGER, Wolters Kluwer, 2006.

[20] L'art. 8, rubricato "Protezione dei dati di carattere personale", stabilisce che: «**1.** *Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano.* **2.** *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 individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica.* **3.** *Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente».*

ISSN 2531-6931

dei dati personali viene riconosciuto autonomo dal diritto al rispetto della propria vita privata e familiare ex art. 7[21].
Nel diritto al rispetto della vita privata e familiare si manifesta soprattutto il momento individualistico. Il potere si esaurisce sostanzialmente nell'escludere interferenze altrui: la tutela è statica, negativa. La protezione dei dati, invece, fissa regole ineludibili sulle modalità del loro trattamento e si concretizza in poteri d'intervento: la tutela è dinamica, segue i dati nella loro circolazione. I poteri di controllo e d'intervento, inoltre, non sono attribuiti soltanto ai diretti interessati, ma vengono affidati anche a una autorità indipendente (ex art. 8.3): *«la tutela non è più soltanto individualistica, ma coinvolge una specifica responsabilità pubblica»*[22], rileva Rodotà.

Se, da un lato, l'art. 8 della Carta di Nizza sancisce il diritto fondamentale alla protezione dei dati personali, dall'altro, l'art. 52 dispone che i diritti fondamentali tutelati dalla Carta non sono assoluti, ma possono essere limitati, con previsione legislativa, per realizzare finalità di interesse generale (e la tutela della salute lo è più che mai) a patto che ciò avvenga tramite di misure proporzionate e che non si intacchi il loro contenuto essenziale.

A quanto detto, si aggiunga che l'art. 16 del Trattato sul funzionamento dell'Unione europea, prescrivendo che *«ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano»*, attua una più intensa tutela del diritto alla protezione dei dati personali.

Sempre sul piano sovranazionale, il diritto alla *privacy* trova riscontro come diritto fondamentale all'art. 12 della Dichiarazione universale dei diritti dell'uomo, ove si legge che *«nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesione del suo onore e della sua reputazione».*

[21] L'art. 7, rubricato "Rispetto della vita privata e familiare", prescrive che: *«Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni».*

[22] *Il mondo nella rete. Quali i diritti, quali i vincoli*, S. RODOTÀ, Laterza, Roma-Bari, 2014, p. 35.

Inoltre, si stabilisce che *«ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni».*

In maniera analoga, l'art. 17 del Patto internazionale sui diritti civili e politici sancisce che *«nessuno può essere sottoposto ad interferenze arbitrarie o illegittime nella sua vita privata, nella sua famiglia, nella sua casa o nella sua corrispondenza, né a illegittime offese al suo onore e alla sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze od offese».* Tale interferenza potrà operare legittimamente quando: a) sia prevista dal diritto interno, nel cui contesto deve sussistere una previsione accessibile, precisa e conforme alle previsioni del Patto; b) assolva a uno scopo legittimi; c) si configuri come necessaria e proporzionale.

Ancora, l'art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, definita quale *leaving instrument* poiché in grado di adattarsi ai mutamenti della società, contempla il diritto alla *privacy* nell'ambito dei diritti di libertà, come diritto di ciascun individuo alla protezione dei dati di carattere personale che lo riguardano e come diritto ad un trattamento dei dati che sia effettuato secondo i principi di lealtà, finalità e proporzionalità[23]. Sulla base dei requisiti previsti per la compressione del diritto alla *privacy* ed elaborati in relazione al precedente art. 17 del Patto, la Corte EDU ha statuito che le lesioni al diritto al rispetto della vita privata possono avvenire solamente qualora la compressione sia: a) prevista dalla legge; b) necessaria a soddisfare una delle esigenze enunciate dalla norma stessa (sicurezza nazionale, ordine pubblico, benessere economico del Paese); c) proporzionata rispetto allo scopo perseguito.

Sul versante interno di matrice costituzionale non si fa, invece, alcun riferimento alla tutela della *privacy*. A lungo la dottrina ha tentato, pertanto, di trovare un aggancio costituzionale, un fondamento dal quale desumere una specifica tutela al diritto *de quo*. Se, da un lato alcuni autori riconducevano il diritto alla *privacy* a varie tutele – si pensi agli

[23] *Ricostruzione normativo-giurisprudenziale del diritto alla privacy*, V. MARIO, in *Salvis Juribus*, http://www.salvisjuribus.it/ricostruzione-normativo-giurisprudenziale-del-diritto-alla-privacy/#_ftn1, ultimo accesso il 7 maggio 2020.

ISSN 2531-6931

artt. 3, 13, 14, 15, 21 – dall'altro lato, altri autori propendevano verso una copertura costituzionale plurima, derivante da più norme. Il dibattito, infine, si è assestato sulla riconducibilità della *privacy* nell'area di applicazione dell'art. 2 Cost., norma che *«riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo sia nelle formazioni sociali ove si svolge la sua personalità»*[24]. Si tratta, tuttavia, come rilevato da Bricola[25], di una previsione che ha natura aperta e che non offre particolari forme di tutela.

Nel panorama giurisprudenziale, è stata la Corte di Cassazione a fornire un contributo notevole in materia: con la sentenza n. 2129 del 1975 (Caso Soraya), la Suprema Corte è giunta alla definizione del diritto alla riservatezza, statuendo che questa protegge *«certe manifestazioni della vita di relazione, a tutte quelle vicende, cioè il cui carattere intimo è dato dal fatto che si svolgono in un domicilio ideale»*. Inoltre, nella sentenza in esame è stato individuato il fondamento costituzionale del diritto alla riservatezza negli artt. 2, 3, 13, 14, 15, 27, 29 e 41 Cost., oltre che nell'art. 8 CEDU, precisando che *«la tutela giuridica deve ammettersi in caso di violazione del diritto assoluto di personalità, inteso quale diritto erga omnes, alla libertà di autodeterminazione nello svolgimento della personalità dell'uomo come singolo»*.

Il caso anzidetto, considerato *leading case*, ha permesso che nell'ordinamento italiano trovasse regolamentazione questa materia. Nel 1998, inoltre, la Suprema Corte è stata chiamata a decidere un nuovo caso sempre in materia di diritto alla riservatezza, affermando

[24] La Corte costituzionale, con la sentenza n. 81 del 1993, tuttavia, ha ravvisato il fondamento costituzionale del diritto alla riservatezza nell'art. 15 Cost., specificando che *«l'ampiezza della garanzia apprestata dall'art. 15 della Costituzione alle comunicazioni che si svolgono tra soggetti predeterminati entro una sfera giuridica protetta da riservatezza è tale da comprendere non soltanto la segretezza del contenuto della comunicazione, ma anche quella relativa all'identità dei soggetti e ai riferimenti di tempo e di luogo della comunicazione stessa»*, http://www.giurcost.org/decisioni/1993/0081s-93.html, ultimo accesso il 9 maggio 2020.

[25] *Prospettive e limiti della tutela penale della riservatezza*, F. BRICOLA, in *Riv. it. dir. proc. pen*., 1967, p. 1094.

l'esistenza di *«un vero e proprio diritto alla riservatezza anche al di fuori delle ipotesi espressamente previste dalla legge ordinaria»*[26].

Successivamente, sulla base della normativa comunitaria (in particolare con l'emanazione della direttiva 95/46/CE), il diritto alla riservatezza è stato riconosciuto, nel nostro ordinamento, tramite la l. 31 dicembre 1996, n. 675 e, successivamente, con il codice in materia di protezione dei dati personali (codice *privacy*, d.lgs. 196 del 2003). Infine, un definitivo riconoscimento si è avuto con il Reg. UE 679/2016 (ed il d.lgs.101/2018 di recepimento, che armonizza la disciplina).

Le direttive europee hanno giocato un ruolo propulsivo nella materia *de qua:* come la Direttiva 95/46/CE sulla tutela dei dati, la Direttiva 2002/58/CE sull'*e-privacy*, modificata nel 2009, la Direttiva 2006/24/CE sulla conservazione dei dati (dichiarata invalida dalla Corte di giustizia dell'Unione europea l'8 aprile 2014 a causa delle gravi interferenze con la vita privata e la protezione dei dati personali), il Regolamento (CE) n. 45/2001 sul trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari nonché, nell'ambito dell'ex terzo pilastro, la Decisione Quadro 2008/977/GAI del Consiglio sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale.

Ad ogni modo, l'Unione europea non ha arrestato il processo evolutivo in materia e, di fatto, ha elaborato nuovi atti, alcuni dei quali hanno modificato il *framework* legale esistente mediante l'introduzione di una nuova disciplina giuridica. Rilevante a tal proposito è il regolamento del 27 aprile 2016, n. 679 (*General Data Protection Regulation*) 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[27].

---

[26] Corte di Cassazione Civile, Sezione III, n. 5658 del 1998 in *Il Foro Italiano,* Vol. 121, n. 9, settembre 1998.

[27] V. MARIO, *art. cit.*

ISSN 2531-6931

Il regolamento costituisce un prezioso tentativo di armonizzazione delle regole *privacy* dei vari Stati ed è finalizzato a sviluppare il mercato unico digitale attraverso la creazione e la promozione di nuovi servizi, applicazioni, piattaforme e *software*. Il regolamento costituisce con la direttiva Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati, il c.d. "pacchetto protezione dati personali"[28].

La *privacy* viene qualificata dal Regolamento 679 presidio irrinunciabile della libertà della persona e allo stesso tempo, indirettamente, interesse generale della società. Come vi si stabilisce, occorre che *«le persone fisiche abbiano il controllo dei dati personali che li riguardano e che la certezza giuridica e operativa sia rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche»* (settimo considerando). Ne consegue che la protezione dei dati personali è espressamente qualificata dal recente Regolamento, non solo come un diritto individuale, ma anche come un interesse pubblico rilevante per le società contemporanee, una garanzia per la loro democraticità e per il loro buon funzionamento[29].

[28] *Regolamento Ue 2016/679, ecco tutto ciò che cittadini e PA devono sapere*, M. ALOVISIO, Agenda Digitale, https://www.agendadigitale.eu/infrastrutture/nuovo-regolamento-privacy-ue-ecco-tutto-cio-che-cittadini-e-pa-devono-sapere/, ultimo accesso il 7 maggio 2020.

[29] *Una rilettura del concetto di sicurezza nell'era digitale e della emergenza normalizzata*, G. DE VERGOTTINI, in *Rivista AIC*, 4/2019, p. 2, https://www.rivistaaic.it/it/rivista/ultimi-contributi-pubblicati/giuseppe-de-vergottini/una-rilettura-del-concetto-di-sicurezza-nell-era-digitale-e-della-emergenza-normalizzata, ultimo accesso il 7 maggio 2020.

§IV. **Salute pubblica vs *privacy*: analisi di un delicato bilanciamento**

È una reazione fisiologica quella degli ordinamenti democratici adottare misure emergenziali e di polizia per fronteggiare minacce alla sicurezza dei propri cittadini. Finora le democrazie occidentali sono state abituate alla minaccia terroristica di matrice islamica incarnata dal Daesh, sebbene, per adesso, sopita. A partire dai primi di gennaio non solo le democrazie occidentali, ma il mondo intero si trovano a dovere affrontare una minaccia epidemiologica rappresentata dal COVID-19 che ha originato un'emergenza sanitaria di portata globale.

In generale, il modo con cui gli ordinamenti reagiscono a situazioni eccezionali si concreta nel ricorso a interventi normativi regolatori di carattere emergenziali che consistono primariamente nell'inasprimento delle misure di polizia e nella compressione di diritti costituzionalmente presidiati.

Le tradizionali libertà negative – a partire dalla libertà personale – sono i primi diritti fondamentali dell'uomo a risultare potenzialmente compressi dall'inasprimento delle misure di sicurezza. In seguito agli attentati terroristici più recenti – quelli post Charlie Hebdo – e all'esperienza attuale di contrasto alla minaccia epidemiologica, invece, sono emerse nuove, ulteriori, sfide. Le esigenze di controllo e prevenzione hanno infatti dei punti di contatto sia con gli ambiti di tutela delle libertà fondamentali nella loro forma di esercizio più classica e tradizionale, sia nella declinazione che si potrebbe definire come "digitale", con riferimento all'impiego dei mezzi di comunicazione soprattutto attraverso la Rete.

Di fronte all'emergenza in atto, i Governi di tutto il mondo hanno deciso di intervenire incisivamente e in un contesto caratterizzato da più elevati livelli di tecnologizzazione e di informatizzazione, che offre nuove sfide sia alle modalità di prevenzione e di controllo della collettività, sia alle limitazioni cui devono essere sottoposti i diritti fondamentali.

ISSN 2531-6931

Ma il potenziamento delle tradizionali misure di polizia è recentemente andato di pari passo con l'introduzione di nuovi strumenti e il rafforzamento delle misure di monitoraggio digitale per finalità di tutela della salute pubblica, che dunque pongono in primo piano la necessità di concentrarsi sulla tutela dei dati personali – a partire dal loro impiego – e sul complesso bilanciamento tra due esigenze: quella statale, di tracciamento della collettività ai fini di contrasto del COVID-19, e quella privata, di mantenimento della sfera giuridica personale inviolata.

Nel nome della lotta contro la pandemia, alcuni Governi si sono affrettati a espandere il loro uso delle tecnologie di sorveglianza per tracciare gli spostamenti di individui e persino intere popolazioni. Se lasciate incontrollate e incontrastate, queste misure hanno il potenziale per alterare radicalmente il futuro del diritto alla *privacy* e degli altri diritti umani.

Nella presente sede, dunque, si tenterà di tracciare il rapporto intercorrente tra il diritto alla *privacy* e alla protezione dei dati personali – diritto fondamentale di ogni individuo – e la tutela della salute pubblica – presidiata all'art. 32 Cost. – alla ricerca di un possibile equilibrio fra le diverse esigenze che consenta di non comprimere oltremodo gli spazi fondamentali nonostante le tendenze restrittive in atto. Si cercherà di riflettere sul bilanciamento dei diritti in gioco e sulla consapevolezza che la prevalenza di un diritto rispetto all'altro non comporta una totale e irragionevole compressione del diritto ritenuto cedevole.

Se, infatti, l'elevata capacità di analisi predittiva e in tempo reale consentita dalle più recenti tecnologie rappresenta una risorsa preziosa e strategica specie in situazioni di emergenza, gli impatti, anche di lungo periodo per i diritti e le libertà degli individui non possono essere sottovalutati.

La portata, così come il rigore delle misure attuate, derogatorie e temporanee rispetto alla disciplina ordinaria, per il contenimento e il

contrasto del diffondersi del virus, estese sull'intero territorio nazionale, sono mosse da un unico intento: tutelare il diritto fondamentale di ognuno alla salute pubblica[30].

Le libertà e i diritti in gioco (libertà di circolazione, di associazione, d'impresa, diritti dei lavoratori, diritto alla protezione dei dati personali, libertà di culto), infatti, sono cedevoli rispetto alla tutela della salute, consacrata all'art. 32[31] della Costituzione repubblicana come fondamentale diritto dell'individuo e interesse della collettività.
Cedevolezza che, tuttavia, non implica sospensione o, addirittura, totale estinzione.

La *privacy* non è né un ostacolo all'efficace azione di prevenzione del contagio né, tantomeno, un lusso cui, secondo taluni, si dovrebbe rinunciare in tempi di emergenza. È un diritto di libertà che, come ogni altro diritto fondamentale, soggetto a bilanciamento con altri beni giuridici, modula la sua intensità e il suo contenuto in ragione dello specifico contesto in cui si eserciti. Si può e si deve certamente tutelare al massimo grado l'incolumità individuale, senza per questo tradire i cardini della democrazia, tra cui in primo luogo il necessario equilibrio tra interessi collettivi e libertà individuali[32].

Precisamente, qualora insorgesse un contrasto (anche potenziale) tra due diritti di pari rango (come lo sono salute e riservatezza) non si può pensare di far prevalere inconfutabilmente l'uno sull'altro, ma occorre effettuare un c.d. "bilanciamento di interessi". Detto

---

[30] *Covid-19, tra diritto alla salute e tutela della privacy: la scelta che l'Italia deve fare*, B. CALDERINI, Agenda Digitale, https://www.agendadigitale.eu/sicurezza/privacy/covid-19-il-difficile-equilibrio-tra-diritto-alla-salute-e-tutela-della-privacy/, ultimo accesso l'8 maggio 2020.

[31] *«La Repubblica tutela la salute come fondamentale diritto dell'individuo e interesse della collettività, e garantisce cure gratuite agli indigenti.*

Nessuno può essere obbligato a un determinato trattamento sanitario se non per disposizione di legge. La legge non può in nessun caso violare i limiti imposti dal rispetto della persona umana».

[32] *Antonello Soro: emergenza Covid-19, le deroghe sul diritto alla privacy non devono diventare un punto di non ritorno*, intervento di A. SORO, Garante per la Protezione dei Dati Personali, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9296264, ultimo accesso il 9 maggio 2020.

ISSN 2531-6931

diversamente, questo vuol dire trovare il giusto equilibrio tra i due diritti, in modo da poter perseguire entrambe le tutele, laddove possibile, o comunque fare in modo che la prevalenza di uno non comporti la cancellazione di altri diritti, in quanto le norme non vanno lette in contrapposizione l'una dell'altra, ma vanno armonizzate in modo da raggiungere lo scopo che si prefigge l'ordinamento, cioè la tutela dei cittadini nell'esplicazione di tutti i diritti che ad essi spettano[33].

Già qualche anno addietro, con la sentenza n. 11994 del 6 maggio 2017, la Corte di Cassazione si è espressa sul caso del contrasto tra diritti o interessi della persona, in particolare quello configurabile tra il diritto alla *privacy* di dati sensibili di natura sanitaria e il diritto alla salute e all'integrità psico-fisica di terzi o della collettività, ritendendo di dover considerare prevalente il diritto all'incolumità fisica della collettività contro il diritto alla difesa dei dati personali[34].

Ma effettivamente, nell'attuale scenario emergenziale, bisogna chiedersi come coniugare e bilanciare il diritto alla *privacy* con la tutela della salute pubblica e, inoltre, se e su che basi comprimere il primo dei diritti. Va, anzitutto, ricostruita la base normativa incidente sul diritto alla *privacy*. Tra le svariate misure adottate, ci si deve soffermare sull'art. 5 dell'Ordinanza del capo dipartimento della Protezione Civile n. 630 del 3 febbraio 2020 e sull'art. 14 del decreto-legge n. 14 del 9 marzo 2020.

---

[33] *Perché l'emergenza Covid-19 non implica la sospensione della privacy*, R. ZALLONE, DirittoPrivacy.it, https://dirittoprivacy.it/perche-lemergenza-covid-19-non-implica-la-sospensione-della-privacy/, ultimo accesso l'8 maggio 2020.

[34] Merita rilievo pure quanto considerato dalla Suprema Corte laddove si afferma che «*…quando il pericolo per il terzo o per la collettività fosse stato sì stringente da configurare la posizione del titolare del trattamento, in relazione alla particolarità della figura dell'operatore e della struttura sanitaria, addirittura come rilevante sotto il profilo della figura civilistica e penalistica dello stato di necessità, si sarebbe potuto dubitare che mancando il consenso dell'interessato la stessa autorizzazione del Garante non fosse necessaria, per la prevalenza dei presupposti di quella figura*». Corte di Cassazione, Sez. III civile, sentenza 16 maggio 2017, n.11994, in Privacy.it, https://www.privacy.it/2017/05/06/cass-privacy-paziente-vs-salute-terzi/, ultimo accesso il 9 maggio 2020.

In merito al trattamento dei dati, l'art. 5 della richiamata ordinanza ha disposto che i soggetti operanti nel Servizio nazionale di protezione civile, unitamente alle Forze dell'Ordine, ai Comuni e soggetti privati autorizzati, possono realizzare trattamenti, ivi compresa la comunicazione tra loro, dei dati personali, anche sensibili, al fine realizzare gli scopi ed i compiti propri della Protezione Civile così come previsto dal decreto legislativo n. 1/2018 (c.d. Codice della Protezione Civile). A ciò si aggiunga che l'art. 14 dell'anzidetto decreto-legge ha ampliato il novero dei soggetti che potranno trattare e comunicare fra loro i dati personali, anche sensibili, fino al termine dell'emergenza sanitaria in atto (31 luglio 2020). Oltre ai soggetti operanti nel Servizio nazionale di protezione civile e gli attuatori dell'o.c.d.p.c. n. 630/2020, vi rientrano gli uffici del Ministero della salute e dell'Istituto Superiore di Sanità, le strutture pubbliche e private operanti nell'ambito del S.S.N. e tutti i soggetti deputati a garantire l'esecuzione delle misure di contenimento della diffusione del virus. A ciò si aggiunga che la comunicazione dei dati personali, con esclusione di quelli sensibili, a soggetti pubblici o privati diversi e ulteriori rispetto a quelli individuati dall'ordinanza e dal decreto-legge, è effettuata se dovesse risultare indispensabile per attuare le misure emergenziali in atto[35].

È certo che, in ogni caso, tutte le attività di trattamento dei dati personali ritenute o previste come necessarie per la gestione dell'emergenza, ai sensi dell'art 14 co. 3 dello stesso decreto-legge, dovranno essere vincolate al rispetto dei principi fissati dal Regolamento europeo n. 679/2016, adottando misure appropriate a tutela dei diritti e delle libertà degli interessati.

Con riferimento al Regolamento citato, si noti che una lettura più attenta del testo consente di affermare che, senza ombra di dubbio, il diritto alla *privacy* non è un diritto assoluto che non conosce limiti, confini e compressioni.

---

[35] *Prove di bilanciamento tra il diritto alla privacy e il diritto alla salute (pubblica)*, G. GIAMMATTEI, in *Salvis Juribus*, http://www.salvisjuribus.it/prove-di-bilanciamento-tra-il-diritto-alla-privacy-e-il-diritto-alla-salute-pubblica/, ultimo accesso il 9 maggio 2020.

ISSN 2531-6931

Se, da un lato, il Considerando 1 del Regolamento *de quo* stabilisce che la protezione delle persone fisiche con riguardo al trattamento dei dati con carattere personale è un diritto fondamentale, dall'altro, i Considerando 16 e 46 dispongono che il presente Regolamento non si applica al trattamento dei dati personali quando vi è in gioco la sicurezza comune dell'Unione Europea, quando è necessario tutelare la vita dell'interessato o di un'altra persona fisica e quando vi sono rilevanti motivi di interesse pubblico tra cui l'evoluzione e la diffusione di epidemie. Inoltre, il Considerando 52 si riferisce specificamente alle deroghe al divieto di trattamento di dati sensibili giustificato a "scopi di monitoraggio e allarme" e "prevenzione o controllo delle malattie trasmissibili e di altre gravi minacce per la salute".

A ciò si aggiunga che secondo l'art. 6 del Reg. citato è sempre lecito il trattamento dei dati personali quando ciò si rende necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica, e, secondo l'art. 9, lett. i Reg. cit. è sempre consentito il trattamento dei dati personali c.d. sensibili quando esso è necessario per motivi di interesse pubblico nel settore della sanità pubblica, come nel caso della protezione da gravi minacce per la salute pubblica di carattere transfrontaliero[36].

Ai sensi dell'art. 23, inoltre, ogni Stato membro, come la stessa Unione Europea, può, in particolari circostanze che richiedono la pronta salvaguardia di importanti interessi pubblici generali, calibrare il contenuto di specifiche limitazioni ai diritti e agli obblighi previsti in materia di trattamento dei dati personali con l'introduzione di specifici provvedimenti funzionali all'introduzione delle richieste misure urgenti. Il criterio valutativo della "stretta" necessità e proporzionalità che legittima ogni variazione del potere di effettuare trattamenti, attuata ai sensi dell' art. 23, prevista sin dai Considerando 4 e 54 ed

[36] *Ibidem*.

espressamente contemplata nell'art. 6 e, nel caso dei dati personali concernenti la salute, i dati biometrici e i dati giudiziari anche dagli artt. 9 e 10, costituisce il nucleo fondamentale dell'equilibrio mobile derivante da quel necessario bilanciamento alla base degli atti di legge emergenziali, delle conseguenti misure attuate e degli obiettivi di contenimento e prevenzione del contagio perseguiti dai medesimi.

Proprio l'individuazione del "contenuto essenziale" del diritto da salvaguardare assume in tal senso un rilievo centrale nell'ottica dell'imposizione del minor sacrificio possibile apportato al diritto soccombente ritenuto nella specifica situazione non preminente. In altre parole, le limitazioni e le estensioni alla possibilità di effettuare i trattamenti, possono ritenersi giustificabili fino al punto in cui si rivelino funzionali alla salvaguardia dell'interesse generale alla salute pubblica valutato come prevalente nella cornice delle tutele espresse nell'art. 8 CEDU e nell'art. 52 della Carta di Nizza[37].

§V. **Attività di *contact tracing* e profili problematici dell'*app* "Immuni"**

L'avvio della discutissima *app* "Immuni" per la lotta alla diffusione del COVID-19 rientra tra i temi più caldi dell'attualità. Si tratta della misura più attesa, fra le tante proposte dall'Esecutivo, e da attuare nella c.d. "Fase 2" dell'emergenza. Di certo, non possono nascondersi le numerose polemiche suscitate in merito ai possibili rischi di violazione della *privacy* e di normalizzazione della sorveglianza, dovuti all'introduzione del sistema di tracciamento dei contatti e dei contagi per mappare, prevenire e reagire tempestivamente alla impetuosa diffusione del COVID-19. La tematica del c.d. *contact tracing*[38] ha aperto

[37] *Covid-19, tra diritto alla salute e tutela della privacy: la scelta che l'Italia deve fare*, B. CALDERINI, Agenda Digitale, https://www.agendadigitale.eu/sicurezza/privacy/covid-19-il-difficile-equilibrio-tra-diritto-alla-salute-e-tutela-della-privacy/, ultimo accesso il 9 maggio 2020.

[38] Il tracciamento dei contatti è una delle azioni di sanità pubblica utilizzate per la prevenzione e il contenimento della diffusione di molte malattie infettive. Rappresenta uno strumento importante

ISSN 2531-6931

profili problematici di natura tecnologica ma soprattutto di natura giuridica.

L'applicazione per le attività di *contact tracing*[39] scelta dal Governo italiano – selezionata tra le oltre 300 soluzioni proposte da privati, società ed enti – è sviluppata dalla società milanese Bending Spoons S.p.a.[40] e dovrebbe assicurare le garanzie del rispetto della *privacy,* escludendo l'invasiva soluzione della tecnologia GPS non aderente alle *guidelines* europee e al principio di minimizzazione consacrato nel Regolamento europeo 679/2016, dato che, inoltre, la finalità ultima dell'*app* è rilevare eventi di contatto con contagiati e non movimenti degli individui.

Venendo brevemente alle caratteristiche pratico-operative dell'*app* va precisato che questa sarà composta da una parte dedicata al *contact tracing* vero e proprio, da operarsi via *Bluetooth*, e dall'altra destinata a ospitare una sorta di "diario clinico" in cui l'utente possa annotare progressivamente i dati relativi alle proprie condizioni di salute, quali

all'interno di una strategia adottata dagli Stati per identificare e segnalare le persone che si presumono contagiate dal COVID-19 e arrestare il focolaio.

[39] Il Garante della *privacy*, con il parere del 29 aprile 2020, ha riconosciuto la conformità del sistema di tracciamento italiano al Regolamento europeo e alle linee guida predisposte il 21 aprile dal Comitato europeo per la protezione dei dati. L'uso dell'*app*, nonché ogni trattamento dei dati personali saranno interrotti alla data di cessazione dello stato di emergenza, cioè il 31 luglio e comunque non oltre il 31 dicembre 2020.

[40] Con l'ordinanza n. 10/2020, del 16 aprile scorso, il Commissario straordinario per l'attuazione e il coordinamento delle misure di contenimento e contrasto dell'emergenza epidemiologica COVID-19 ha disposto di procedere alla 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 in relazione all'*app* "Immuni". *Luci e ombre sulla procedura di selezione di "Immuni", l'app del governo di tracciamento del contagio da Covid-19*, P. CLARIZIA, E. SCHNEIDER, IRPA, https://www.irpa.eu/luci-e-ombre-sulla-procedura-di-selezione-di-immuni-lapp-del-governo-di-tracciamento-del-contagio-da-covid-19/, ultimo accesso il 9 maggio 2020. Gli autori, a questo proposito, si interrogano sulla compatibilità della gratuità con la configurazione del rapporto in termini di appalto, contraddistinto dalla necessaria onerosità e sinallagmaticità delle prestazioni. Rilevano, pertanto, che il rapporto sembrerebbe piuttosto inquadrabile come una sponsorizzazione (se si valorizza il ritorno di immagine e la possibilità di acquisire vantaggi nella fase di sviluppo e attuazione dell'*app*), o come una donazione (nei limiti della possibilità di donazione di cosa futura).

la presenza di sintomi compatibili con il virus. L'applicazione si fonda sulla tecnologia *Bluetooth Low Energy* e mantiene i dati dell'utente sul proprio dispositivo, assegnandogli un ID temporaneo, che varia continuamente e viene scambiato tramite *Bluetooth* con i dispositivi vicini. Quanto, invece, al tracciamento vero e proprio: 1) i cellulari conservano in memoria i dati di altri cellulari con cui sono entrati in contatto, in forma di codici anonimi crittografati; 2) quando uno dei soggetti che ha scaricato l'*app* risulta positivo al virus, gli operatori sanitari gli forniscono un codice di autorizzazione con il quale questi può scaricare su un *server* ministeriale il proprio codice anonimo; 3) cellulari con l'*app* prendono dal server i codici dei contagiati; 4) Se l'*app* riconosce tra i codici nella propria memoria un codice di un contagiato, visualizza la notifica all'utente[41].

Gli sviluppatori di "Immuni", di concerto con il Ministero dell'Innovazione, hanno deciso di modificare in corso d'opera il modello di funzionamento, per innalzare i livelli di *privacy* e la sicurezza dei dati. Si seguono le idee del progetto *Decentralised Privacy-Preserving Proximity Tracing* (DP-3T) perseguendo un modello più decentralizzato che mantiene l'allocazione dei dati sul *device* del singolo che ha aderito al sistema di *tracing*. Così, ogni volta che due cellulari si "incontrano" si scambiano il proprio identificativo anonimo generato localmente con crittografia. Dunque, il cellulare dotato dell'*app* porta con sé soltanto una lista di numeri privi di qualsiasi elemento identificativo della persona[42].

Quanto all'utilizzo dell'*app* da parte dell'utente, come rilevato dal Garante italiano per la protezione dei dati personali, questo dovrà avvenire su base volontaria in ragione dell'impossibilità di imporre l'utilizzo di dispositivi elettronici nello specifico alle fasce della

[41] *Immuni, cos'è e come funziona l'app italiana coronavirus*, R. BERTI, Agenda Digitale, https://www.agendadigitale.eu/cultura-digitale/immuni-come-funziona-lapp-italiana-contro-il-coronavirus/, ultimo accesso il 9 maggio 2002.

[42] *Ibidem*.

popolazione a cui tali strumenti, ovvero il cui uso quotidiano degli strumenti in questione può dirsi tutt'altro che scontato.

Si segnala, a questo proposito, un'importante criticità concernente il *digital divide*. Secondo uno studio del Financial Times, infatti, si escluderebbero diversi segmenti della popolazione come chi non possiede uno *smartphone* (spesso anziani, meno abbienti) o chi dispone cellulari obsoleti con sistemi operativi non aggiornabili. Perciò, non vi è solo il rischio di aumentare il *divario digitale* tra regioni, paesi o fasce della popolazione, ma anche di non avere una copertura minima necessaria affinché la tracciabilità abbia effetto. Si pensi al caso italiano: si stima che per essere efficace Immuni dovrebbe essere scaricata ed utilizzata almeno dal 60% della popolazione. Considerato che il 71% degli italiani possiede uno *smartphone*, significa che almeno l'85% di questi debba scaricare l'*app* di tracciabilità[43].

In soccorso alle Autorità, nello svolgimento della delicata attività di bilanciamento degli interessi e di adozione di misure di contenimento del contagio che possano risultare efficaci, il Comitato europeo per la protezione dei dati (*European Data Protection Board*, d'ora in avanti EDPB) ha fornito delle linee guida inerenti proprio al trattamento da parte delle Autorità pubbliche di dati personali nel contesto di una emergenza sanitaria globale come quella attuale. L'aspetto fondamentale dell'intervento dell'EDPB ha riguardato la coesistenza della tutela della salute e la tutela della riservatezza all'interno dell'attuale panorama normativo, senza alcun bisogno di "sospendere la *privacy*".

L'EDPB, con specifico riferimento all'uso dei dati provenienti dai dispositivi mobili, ha allertato le Autorità sulle misure di sicurezza da applicare agli stessi affinché il trattamento non sia lesivo dei diritti

[43] *Nel ginepraio delle app di tracciabilità*, S. DOMINIONI, ISPI, https://www.ispionline.it/it/pubblicazione/nel-ginepraio-delle-app-di-tracciabilita25873?fbclid=IwAR2XjZqO9xw2BUA7FmGGz9wGssMaQLAhkMHtQpRtvCZBCzEdyPmJG3vB_Co, ultimo accesso il 9 maggio 2020.

personali e non costituisca un rischio sproporzionato. Si applica, pertanto, al trattamento di tali dati anche il principio di proporzionalità: nel momento in cui lo Stato deve decidere quale soluzione adottare, deve sempre preferire quella che consente di ottenere uno specifico obiettivo per mezzo della minore intrusione nella sfera personale dei cittadini. Si dovranno implementare, pertanto, meccanismi che siano proporzionati, che corrispondano ad esigenze davvero necessarie e adeguate al rischio, con misure che risultino le meno invasive possibile, nel rispetto dei principi di finalità e minimizzazione del dato di cui sarà necessario anche garantire la sicurezza. Sarà anche importante che qualunque scelta si decida di compiere in merito a controlli o tracciamenti non sia irreversibile ma necessariamente limitata nel tempo, potendo essere "disinnescata" quando la finalità di contenimento dell'epidemia sia venuta meno.[44]

In dottrina è stato rilevato [45] incisivamente che il ricorso al trattamento dei dati personali e sanitari, nel contesto delle attività di *contact tracing*, dovrà operare nel rispetto di requisiti quali:

- → **Formalità**: le interferenze devono essere previste da una base giuridica variamente intesa;
- → **Indispensabilità**: le interferenze devono essere necessarie nel quadro di una società democratica;

[44] Come messo in luce da Antonello Soro, citato in *Contact tracing vs il coronavirus, dove va l'Europa: le app dei diversi Paesi*, M. R. CARBONE, Agenda Digitale, https://www.agendadigitale.eu/sicurezza/privacy/contact-tracing-vs-il-coronavirus-dove-va-leuropa-le-app-dei-diversi-paesi/, ultimo accesso il 9 maggio 2020, *«la chiave è nella proporzionalità, lungimiranza e ragionevolezza dell'intervento, oltre che naturalmente nella sua temporaneità. Il rischio che dobbiamo esorcizzare è quello dello scivolamento inconsapevole dal modello coreano a quello cinese, scambiando la rinuncia a ogni libertà per l'efficienza e la delega cieca all'algoritmo per la soluzione salvifica. Così, una volta cessata quest'emergenza, avremo anche forse imparato a rapportarci alla tecnologia in modo meno fideistico e più efficace, mettendola davvero al servizio dell'uomo».*

[45] *La tempesta perfetta covid-19, deroghe alla protezione dei dati personali ed esigenze di sorveglianza di massa*, G. DELLA MORTE, SIDIBlog, http://www.sidiblog.org/2020/03/30/la-tempesta-perfetta-covid-19-deroghe-alla-protezione-dei-dati-personali-ed-esigenze-di-sorveglianza-di-massa/, ultimo accesso il 9 maggio 2020.

- → **Finalità**: le interferenze devono corrispondere allo scopo di protezione della salute;
- → **Tassatività**: le interferenze devono essere specificate nel modo più dettagliato;
- → **Temporalità**: le interferenze devono indicare il periodo di vigenza;
- → **Impugnabilità**: le interferenze devono essere contestabili in qualche forma;
- → **Proporzionalità**: le interferenze non devono mai essere eccessive rispetto allo scopo perseguito.

Ulteriori profili problematici che sono stati sollevati attengono alla gestione dei dati personali da parte di soggetti pubblici e la dislocazione sul territorio italiano dei *server* ospitanti tali dati. Autorevolmente, a tal riguardo, è stato evidenziato da Mele[46] che *«chi conserverà i dati sanitari dei cittadini, che comunicheranno attraverso l'applicazione di essere risultati positivi al COVID-19, lo faccia utilizzando server dislocati solo sul territorio italiano, in modo da non rendere disponibili i dati a soggetti terzi che potrebbero essere tentati di farne un uso per finalità ulteriori»* lucrative. Inoltre, auspicando la c.d. sovranità digitale per la gestione del *contact tracing* di Stato, la dottrina appena citata ha rilevato che *«la gestione di questi dati dei cittadini non potrà che essere affidata ad un soggetto pubblico italiano»* ossia amministrazioni o enti pubblici o società a totale partecipazione pubblica.

§VI. **"Infodemia" da COVID-19**

[46] *Immuni, il giudizio di esperti: "Con sovranità digitale? Se non obbligatoria non serve a nulla. È open source?"*, L. GAROFALO, Key4Biz, https://www.key4biz.it/immuni-il-giudizio-di-esperti-con-sovranita-digitale-se-non-obbligatoria-non-serve-a-nulla-e-open-o-no-e-le-vulnerabilita-del-bluetooth/300883/, ultimo accesso il 9 maggio 2020.

«Non stiamo lottando solo contro un'epidemia ma anche contro un'infodemia»[47] aveva già esclamato a febbraio il Direttore Generale dell'Organizzazione Mondiale della Sanità, Tedros Adhanom Ghebreyesus, illustrando l'eccessiva massa di informazioni sulla questione, che rende ardua la possibilità di individuare una soluzione. La c.d. "infodemia", cui concorrono disinformazione, false notizie, voci infondate, può compromettere una corretta ed efficace risposta di sanità pubblica oltre a creare confusione e diffidenza tra la gente.

La sovrabbondanza di informazioni o bulimia informazionale – tra cui alcune false o imprecise, provenienti da fonti diverse e dal fondamento spesso non verificabile – sul virus, sulla sua origine e sui suoi effetti, come pure sulle azioni delle autorità per contrastare la pandemia, sta rendendo difficile per i cittadini trovare le fonti e gli orientamenti affidabili di cui hanno bisogno.

La pandemia è una situazione particolarmente rischiosa anche per quanto riguarda il diffondersi di varie tipologie di "*information disorder*": letteralmente "disturbi dell'informazione" che si manifestano sotto forma di disinformazione o misinformazione.

Una precisazione è necessaria. Mentre la "misinformazione" rappresenta una peculiare forma di disinformazione, in cui la divulgazione di contenuti non veritieri non presuppone alcun intento malevolo, le campagne di "disinformazione" comportano la produzione e/o la diffusione intenzionale di contenuti falsi, sensazionali, scandalistici a fini devianti. La condivisione di notizie false, specie sui *social network* può collegarsi a un'attività politica "paramilitare", all'amplificazione di confusione e di discussioni futili al fine di destabilizzare il quadro di riferimento[48].

---

[47] *UN tackles 'infodemic' of misinformation and cybercrime in COVID-19 crisis*, The United Nations Department of Global Communications, UNITED NATIONS, https://www.un.org/en/un-coronavirus-communications-team/un-tackling-'infodemic'-misinformation-and-cybercrime-covid-19, ultimo accesso l'8 maggio 2020.

[48] *Tecnologie per il potere. Come usare i social network in politica*, G. ZICCARDI, Raffaello Cortina Editore, Milano, 2019, p. 197.

ISSN 2531-6931

Il c.d. "contagio informativo" ha l'effetto di rendere assai più complessa la gestione dell'emergenza, in quanto pregiudica la possibilità di trasmettere istruzioni chiare e univoche e di ottenere, quindi, comportamenti omogenei da parte della popolazione. Ciò marca una differenza epocale rispetto alle emergenze globali, non solo sanitarie, del passato, quando la maggior lentezza di trasmissione delle notizie e il numero limitato di mezzi di comunicazione permettevano di reagire in modo più ordinato.

A generare il panico nella popolazione non è solo la dimensione sanitaria del COVID-19, ma anche quella immateriale del contagio che avviene attraverso *fake news*, disinformazione e incoerenza delle dichiarazioni delle autorità. Lo ha affermato e dimostrato il gruppo di lavoro della Società Italiana di *Intelligence* che ha condotto una ricerca sul tema dal titolo "*La pandemia immateriale. Gli effetti del Covid-19 tra social asintomatici e comunicazione istituzionale*".

Nello spazio cibernetico, in cui la maggior parte della popolazione è costretta a vivere "forzatamente", *«la disinformazione si propaga con la stessa aggressività del virus biologico, attraverso la condivisione collettiva di narrazioni frammentate e incoerenti, il più delle volte false e molto spesso all'insaputa di chi le trasmette. Tutto ciò determina il manifestarsi di uno stato di ansia permanente, alimentando un panico diffuso che limita una più serena valutazione della realtà»*, rilevano gli autori della ricerca[49].

Nell'infodemia da COVID-19, la cattiva informazione si è manifestata in vari modi. Il *Reuters Institute for the Study of Journalism* (RISJ) dell'Università di Oxford ha pubblicato uno dei primi studi sulle caratteristiche della pandemia, concentrandosi su un campione di notizie in lingua inglese vagliate da iniziative di *fact-checking* come il *network* no-profit First Draft. Lo studio rivela come la varietà delle fonti

[49] *La pandemia immateriale. Gli effetti del Covid-19 tra social asintomatici e comunicazione istituzionale*, M. CALIGIURI, L. GIUNGATO, in SOCIETÀ ITALIANA DI INTELLIGENCE, https://press.socint.org/index.php/home/catalog/book/4, ultimo accesso l'8 maggio 2020.

di disinformazione e misinformazione sulla pandemia possano essere sia "*top-down*" (quando sono promosse dalla politica o da altre personalità pubbliche) o "*bottom-up*", ossia quando partono dagli utenti comuni. Se la prima tipologia rappresenta il 20% del totale del campione analizzato dal RISJ, è anche vero però che la disinformazione *top-down* tende a generare molto più consensi sui social media rispetto a quanto prodotto dal basso. Rileva il RISJ, inoltre, che la fetta più grande della misinformazione emersa in queste settimane sarebbe costituita da contenuti "riconfigurati", modificati ovvero in alcune loro parti. Solo una minoranza (il 38% circa) sarebbe invece composta da contenuti completamente inventati ex novo[50].

Passiamo brevemente in rassegna il ruolo della disinformazione statale nel contesto emergenziale globale.

Stando alla relazione speciale del Servizio europeo per l'azione esterna (SEAE), abilitato a gestire le relazioni diplomatiche dell'UE con altri Paesi al di fuori dell'UE e a condurre la politica estera e di sicurezza dell'Unione europea *«sia nell'UE che altrove, l'obiettivo dei messaggi coordinati di disinformazione è imputare a minoranze vulnerabili la responsabilità della pandemia e alimentare la sfiducia nella capacità delle istituzioni democratiche di fornire risposte efficaci. Alcuni attori statali e sostenuti dallo Stato cercano di sfruttare la crisi della sanità pubblica per servire i propri interessi geopolitici, spesso mettendo direttamente in discussione la credibilità dell'Unione europea e dei suoi partner»* [51] . In questo caso, alcune delle informazioni false sul coronavirus, che contribuiscono ad alimentare tale infodemia di portata globale, sono state create da forze politiche specifiche tra cui Cina e Russia. In questi casi l'obiettivo è politico: indebolire l'Unione Europea o creare cambiamenti politici, indurre sfiducia nelle autorità nazionali ed europee e nei sistemi sanitari e istituzioni internazionali,

[50] *I quattro nemici (quasi) invisibili nella prima pandemia dell'era della società dei dati*, P. DI SALVO, S. MILAN, Il Manifesto, https://ilmanifesto.it/i-quattro-nemici-quasi-invisibili-nella-prima-pandemia-dellera-della-societa-dei-dati/, ultimo accesso l'8 maggio 2020.

[51] *Contrastare la disinformazione*, CONSIGLIO DELL'UNIONE EUROPEA, https://www.consilium.europa.eu/it/policies/covid-19-coronavirus-outbreak-and-the-eu-s-response/fighting-disinformation/, ultimo accesso l'8 maggio 2020.

ISSN 2531-6931

enfatizzando la capacità dei sistemi non democratici – quali la Russia – di contenere la diffusione del virus.

Inoltre, il *National Security Council* americano ha puntato il dito contro la disinformazione di Stato russa sul coronavirus. L'amministrazione Trump ha, infatti, imputato alla regia del Cremlino un'operazione di disinformazione globale sulle origini e la natura della pandemia del COVID-19. A inizio febbraio, in particolare, i media governativi e filo-governativi russi hanno iniziato a concedere ampio spazio ad alcune teorie complottiste secondo cui il coronavirus sarebbe in realtà un prodotto di laboratorio degli Stati Uniti. Precisamente, si è sostenuto che il coronavirus sarebbe un'"arma bio-etnica" degli americani[52].

Tali messaggi disinformativi sono caratteristici della strategia consolidata del Cremlino di utilizzare la disinformazione per amplificare le divisioni, seminare diffidenza e il caos e aggravare le situazioni di crisi e le questioni di interesse pubblico.

Autorevolmente è stato rilevato da Rid, nell'ambito del rapporto tra le operazioni di disinformazione e la sicurezza nazionale, che la situazione di pandemia possa costituire anche un terreno particolarmente fertile per potenziali operazioni di *information warfare*[53] volte a creare confusione e tensioni nelle opinioni pubbliche dei Paesi colpiti, sulla scia di quanto si è visto negli Stati Uniti durante le elezioni presidenziali del 2016.

---

[52] *La disinformazione ai tempi del Covid-19? La Cia ricorda i vecchi tempi (attuali) del Kgb*, F. BECHIS, in *Formiche*, https://formiche.net/2020/04/disinformazione-tempi-covid19-cia-vecchi-tempi-kgb/, ultimo accesso l'8 maggio 2020.

[53] Secondo la definizione tratta da *Glossario Intelligence. Il linguaggio degli Organismi informativi*, SISTEMA DI INFORMAZIONE PER LA SICUREZZA DELLA REPUBBLICA, 2019, *«il termine indica le azioni intraprese al fine di acquisire superiorità nel dominio informativo minando i sistemi, i processi ed il patrimonio informativo dell'avversario e difendendo al contempo i propri sistemi e le proprie reti nonché, più in generale, l'impiego delle informazioni ai fini del perseguimento degli interessi nazionali. Così concepita, include anche una serie di attività tipiche della tradizione intelligence – ma che oggi possono avvalersi delle potenzialità offerte dal progresso tecnologico – quali la disinformazione, l'influenza e la controinformazione, appartenenti alla categoria delle cd. "psycological operations"».*

La narrativa più ricorrente delle campagne di disinformazione attuali è quella secondo la quale il virus è un'arma biologica creata dall'Occidente – dalla CIA, dalla NATO, dagli Stati Uniti, dall'Inghilterra – per isolare la Cina, per provocare una Sinofobia, per muovere una guerra ibrida contro la Cina, per indebolirla economicamente, per fare fuori la Russia, la Cina o più in generale gli avversari degli Stati Uniti.

Le *fake news* sul COVID-19, tuttavia, non provengono solamente dalla Russia. Una vasta operazione di disinformazione è stata orchestrata dai servizi di *intelligence* cinesi mirata a diffondere il panico negli Stati Uniti per il coronavirus. L'Europa, inoltre, è stata investita da messaggi che enfatizzavano da un lato le divisioni dei Paesi membri di fronte all'emergenza e, dall'altro, l'importanza degli aiuti inviati dalla Cina. In Turchia, Fatih Erbakan, un predicatore e politico islamista vicino al presidente Recep Tayyip Erdogan, ha affermato pubblicamente che il sionismo potrebbe giocare un ruolo nella diffusione del coronavirus. Nella regione del Medio Oriente e del Nord Africa, l'epidemia è stata utilizzata da autorità e organizzazioni terroristiche per far progredire le agende geopolitiche. Si pensi a Daesh che ha sfruttato gli *hashtag* di tendenza (compresi quelli sul coronavirus) per diffondere i propri messaggi per finalità di propaganda. Inoltre, Il coronavirus è stato usato per fomentare il discorso dell'odio e alimentare lo scontro sunnita-sciita nella regione.
Anche alcuni media iraniani legati al governo, come PressTV – un servizio di notizie in inglese e francese – stanno sostenendo la teoria che il coronavirus sia un'arma biologica prodotta dagli USA.

In Conclusione, in Italia, le "bufale" nostrane più disparate sul coronavirus si diffondono su diversi canali, tra cui WhatsApp: dal complottismo che vede le case farmaceutiche produttrici di vaccini come responsabili del virus ai rimedi o regimi alimentari miracolosi che

donano immunità, il panorama italiano è segnato dalle numerose notizie false sulla pandemia[54].

§VII. **Modelli di gestione della *privacy*: una prospettiva comparata**

Gli Stati sono attori primari nella strategia contro il COVID-19. L'utilizzo di strumenti tecnologici per far fronte all'emergenza si sta ormai diffondendo progressivamente. Nella maggior parte dei casi si tratta di strumenti di matrice pubblicistica, in cui lo Stato mette a disposizione le *app*. In alcuni casi, come in Italia, lo Stato ha scelto l'*app* di un soggetto privato nazionale - "Immuni", di *Bending Spoons* - che ha offerto il servizio in modo gratuito, sollevando, tuttavia, numerose questioni.

Le tecniche utilizzate per tracciare il contagio del COVID-19 comportano – lo si è visto – una difficilissima opera di bilanciamento tra il diritto alla salute e il diritto alla riservatezza. Se il primo sembra prevalere nell'immediato, non vanno sottovalutati i rischi futuri derivanti dall'utilizzo esteso di tecniche di controllo del singolo.

Proprio a questo riguardo e, dunque, entrando più nel vivo della vita degli individui, si mettono in discussione misure di controllo di spostamenti e contatti, nel tentativo di realizzare un tracciamento effettivo e di dominare la diffusione del COVID-19 tramite la ricostruzione della catena di contagio.

Tra i modelli di gestione del tracciamento collettivo si è distinto quello della **Corea del Sud**. A fronte di una massiccia campagna di tamponi, lo Stato in esame ha richiesto ai propri cittadini l'utilizzo di

[54] *Coronavirus in Russia: guerra al contagio o contagio dell'informazione?*, E. TAFURO AMBROSETTI, ISPI, https://www.ispionline.it/it/pubblicazione/coronavirus-russia-guerra-al-contagio-o-allinformazione-25456, ultimo accesso l'8 maggio 2020.

un'applicazione di *geotracking* in grado di monitorare ogni spostamento del possessore del *device*. In questo modo, è stato possibile controllare le azioni dei soggetti contagiati, sino ad ottenere sul proprio dispositivo un *alert* in loro prossimità, ossia entro 100 metri. L'*app* "Corona100m", sviluppata dal Ministero dell'Interno e della Sicurezza, permette a chi ha ricevuto l'ordine di non uscire di casa di rimanere in contatto con gli assistenti sociali e di riferire i propri progressi. Mediante l'*app* viene utilizzato anche il GPS per tenere traccia della loro posizione per assicurarsi che non stiano violando la quarantena. Il servizio, è denominato "auto-quarantena di sicurezza". Sono state raccolte anche ulteriori informazioni: sono stati tracciati gli accessi agli ambulatori e alle farmacie, le transazioni delle carte di credito, le registrazioni delle videocamere di sorveglianza. Un monitoraggio, questo, che ha consentito di ottenere in breve tempo una effettiva riduzione del numero di contagiati, seppur con evidente compressione delle libertà dei cittadini tra cui la *privacy*[55]. La Corea del Sud diventata un punto di riferimento nel dibattito corrente, perché ha contenuto la diffusione evitando il *lockdown* nazionale. Secondo le attuali linee guida dei centri coreani per il controllo e la prevenzione delle malattie, chiunque sia entrato in contatto con un portatore di coronavirus confermato è soggetto ad un'auto-quarantena obbligatoria di due settimane. I soggetti in isolamento sono assegnati a un funzionario del governo locale, che controlla telefonicamente due volte al giorno lo sviluppo di eventuali sintomi.

Secondo Privacy International, ONG inglese che si occupa di diritto alla privacy, *«la Corea del Sud non ha mai spiegato il modo in cui le informazioni sono state utilizzate e se quelle raccolte tramite il GPS dei cellulari abbiano davvero fatto la differenza, quindi nessuno ha la prova che i dati sulla posizione abbiano effettivamente contribuito a contenere il virus».*

---

[55] *COVID-19 e norme sul trattamento dei dati sanitari: il GDPR e il modello coreano*, V. COLAROCCO, 4C Legal, https://www.4clegal.com/hot-topic/covid-19-norme-trattamento-dati-sanitari-gdpr-modello-coreano#_ftn1, ultimo accesso l'8 maggio 2020.

ISSN 2531-6931

In Corea - come è stato messo in luce[56] - *«la maggior parte delle persone sembra aver accettato una parziale erosione della propria privacy a condizione di essere informati e di ricevere dati trasparenti. Un patto di fiducia basato su un altissimo tasso di consapevolezza civica, senso di comunità e cooperazione volontaria a sostegno degli sforzi governativi, elementi che certamente hanno anche origine nella concezione del rapporto con l'autorità della cultura confuciana».* È così che in Corea le autorità hanno potuto estrarre, senza mandato, filmati di sorveglianza, lo storico delle carte di credito e i dati di geolocalizzazione delle celle telefoniche dei cellulari dei pazienti già confermati e dei potenziali infetti.

La **Repubblica Popolare Cinese**, da cui ha avuto inizio la pandemia COVID-19, ha risposto efficacemente all'emergenza, risultando in grado di arginarla soprattutto grazie all'utilizzo di tecnologie moderne. Per far fronte al coronavirus, la Cina ha rafforzato il suo già massiccio sistema di sorveglianza dando origine a un sistema pervasivo ubiquitario.

La Cina iniziò a riformare ed aggiornare le sue strutture di *intelligence* all'inizio degli anni 2000 con l'intento di ristabilire il "dominio dell'informazione" su una società sempre più fluida e tecnologicamente sofisticata. Lo Stato ha dimostrato come si sia adattato allo sviluppo tecnologico trasformando e adeguando alle potenzialità offerte dalle nuove tecnologie le proprie procedure di raccolta, analisi e diffusione delle informazioni fino a dare forma all'attuale sistema di *intelligence* di pubblica sicurezza[57].

[56] *App coronavirus: perché la Corea non può essere un modello per l'Italia*, L. FILIOS, Osservatorio Diritti, https://www.osservatoriodiritti.it/2020/04/02/app-coronavirus-italia-corea/, ultimo accesso l'8 maggio 2020.

[57] *Sorveglianza di massa in Cina, il modello che spaventa l'Occidente*, B. CALDERINI, Agenda Digitale, https://www.agendadigitale.eu/sicurezza/privacy/sorveglianza-di-massa-in-cina-cosi-funziona-il-modello-che-spaventa-loccidente/, ultimo accesso l'8 maggio 2020.

Un'immensa rete di sorveglianza copre le città cinesi e conferisce alla polizia poteri quasi illimitati. Conversazioni via *smartphone*, espressioni del volto e movimenti vengono controllati costantemente grazie a un potente sistema di tecnologie integrate gestite da applicazioni di Intelligenza Artificiale. Ecco com'è realizzato uno dei più grandi apparati di spionaggio del mondo, che agisce a scapito della *privacy*. Uno dei diritti privi di copertura costituzionale e tranquillamente conculcato dalle autorità cinesi è quello relativo alla protezione dei dati personali.

Lo sfruttamento di intelligenza artificiale, *Big Data*, robotica, conferma ancora una volta l'indiscusso primato della Cina nello sviluppo e nell'impiego di tali metodologie. Il coronavirus è divenuto catalizzatore per un'ulteriore espansione del regime di sorveglianza, che si perfeziona ad ogni evento particolare alzando ancor più l'asticella: a partire dalle Olimpiadi del 2008 tenutesi a Pechino o all'Expo di Shanghai nel 2010.

Si assiste, in prima battuta, ad un incremento delle già diffusissime (circa 200 milioni) telecamere di sorveglianza, sparse per tutta la Cina, utilizzate per obbligare i cittadini a rispettare la quarantena e per monitorare i movimenti del virus. Le telecamere intelligenti, inoltre, sono applicate anche per "scansionare termicamente" le persone, nonché per identificare i soggetti che non utilizzano le mascherine. La localizzazione e l'isolamento dei focolai grazie alle nuove tecnologie hanno consentito di limitare fortemente il contagio.

Per quel che concerne le scansioni termiche, oltre alle telecamere, sono state adottate anche altre misure. Si tratta di metodi rapidi e particolarmente sicuri di rilevazione della temperatura, come, a titolo esemplificativo, l'utilizzo di TAC che permettono in circa 20 secondi di rilevare nuovi casi di COVID-19, con un'accuratezza che raggiunge il 96% dei casi.

Sono stati impiegai, inoltre, dalla polizia cinese i c.d. "caschi intelligenti" in grado di rilevare la temperatura dei soggetti in un raggio di 5 metri. Le svolte principali, tuttavia, derivano dall'utilizzo dello *smartphone* e di applicazioni di nuova creazione per mano del

ISSN 2531-6931

Governo per il controllo del contagio. Una di queste, denominata *Alipay Health Code*, consente di assegnare ad ogni cittadino un colore – verde, giallo e rosso –, per indicare i soggetti che possono liberamente circolare negli spazi pubblici, quelli con problemi di salute e chi invece ha l'obbligo di restare a casa, in quarantena. Le persone con queste *app* potevano esibire ai posti di blocco e di accesso alle stazioni un codice cromatico (rosso, giallo o verde) che ne attestava lo stato di salute, permettendo al personale di guardia di selezionare i passaggi. Il maggior operatore telefonico del Paese – *China Mobile* – invece, ha condiviso gli spostamenti dei soggetti colpiti dal virus, consentendo la tracciabilità delle linee di contagio.

Persino l'impiego di droni è risultata un'arma importante nella lotta al COVID-19. Una tecnologia di questo tipo ha permesso, infatti, a questi veicoli aerei senza pilota di consegnare cibo e beni di prima necessità ai soggetti in quarantena e campioni medici da un luogo ad un altro, limitando al massimo le occasioni di contatto e, quindi, di contagio. I droni sono utilizzati, inoltre, per pattugliare gli spazi pubblici. La consegna di cibo e medicinali "a distanza" è resa possibile anche grazie all'impiego di *robot*, che si occupano persino della pulizia delle strade[58].

Israele, uno Stato da oltre 45 anni in guerra, ha fatto quello che è egregiamente capace di fare: attivato e applicato lo stato di straordinario di guerra ove il nemico non sta più oltre la striscia di Gaza ma all'interno del suo stesso territorio. Dopo la registrazione del primo caso di COVID-19, datato 21 febbraio scorso, il governo di Tel Aviv aveva imposto la quarantena ad un gruppo di turisti di ritorno da una crociera internazionale sulla nave Diamond Princess. Il 15 marzo ha ordinato il distanziamento sociale in tutto il Paese, mobilitando ufficialmente lo Shin Bet (l'agenzia di *intelligence* per gli affari interni)

[58] *La Cina combatte il Coronavirus con l'IA*, C. RAMOTTI, IRPA, https://www.irpa.eu/la-cina-combatte-il-coronavirus-con-lia/, ultimo accesso l'8 maggio 2020.

per la raccolta di dati dai telefoni cellulari privati onde facilitare il tracciamento delle relazioni sociali tra i contagiati[59].

Israele ha permesso l'applicazione ai cittadini di tecniche di sorveglianza tipiche della lotta al terrorismo. Non a caso l'ente autorizzato a tal fine è stato l'apparato dei servizi di sicurezza Shin Bet. Il Governo, con una misura varata prima delle decisioni del Knesset, ha dato l'autorizzazione al tracciamento su vasta scala tramite tecnologie di sorveglianza, rassicurando comunque il trattamento dei dati personali a fini sanitari.

Si tratterebbe di un programma per ricostruire gli spostamenti dei soggetti che risultino positivi al COVID-19 mediante la geolocalizzazione. Oltre a questo, si garantirebbe che i positivi non violino il periodo di isolamento a casa. Il procuratore generale avrebbe già dato la propria approvazione alle misure speciali, mentre i servizi segreti hanno garantito che non verrà violata la *privacy* e le informazioni non saranno sfruttare per imporre la quarantena, ma dovrebbero servire a ricostruire la mappa degli spostamenti degli infettati. Nonostante ciò deve evidenziarsi che la geolocalizzazione dei telefoni sembrerebbe possa garantire un livello di granularità abbastanza preciso nelle località urbane e il fatto che questo venga presentato come uno strumento di *intelligence* antiterrorismo suggerisce che si tratta di qualcosa di più di una semplice soluzione di base a livello di polizia, più di una semplice *geofencing*[60].

---

[59] *Se contro il virus si mobilita il Mossad (e non solo). Analisi del prof. Teti*, A. TETI, in *Formiche*, https://formiche.net/2020/04/mossad-coronavirus-israele-intelligence/, ultimo accesso l'8 maggio 2020.

[60] *Lotta al coronavirus, Paese che vai privacy che trovi: i diversi approcci (Europa, Cina, Corea, Israele)*, N. MONTE, G. VACIAGO, Agenda Digitale, https://www.agendadigitale.eu/sicurezza/privacy/lotta-al-coronavirus-paese-che-vai-privacy-che-trovi-i-diversi-approcci-europa-cina-corea-israele/ ultimo accesso l'8 maggio 2020.

Un *geofence* (letteralmente: recinzione) è un perimetro virtuale associato a un'area geografica del mondo reale. L'attività di *geofencing*, prevede l'utilizzo di dispositivi capaci di determinare la propria posizione (*location-aware*), si pensi a *smartphone*, usati come terminali di un *location-based service* (LBS). Ad es., in un servizio di questo tipo, quando un utente entra o esce da un *geofence*, il dispositivo oppure il gestore del servizio ricevono una notifica, che può essere usata per controllare azioni

ISSN 2531-6931

Il modello israeliano, nel ricorrere a strumenti di *intelligence*, sembrerebbe, pertanto, sacrificare considerevolmente il diritto alla *privacy*.

Il ricorso a questo tipo di sorveglianza, di solito riservata ai palestinesi, ha acceso un forte dibattito nell'opinione pubblica israeliana. La Corte Suprema di Israele si è espressa a riguardo, dichiarando la necessità che il governo adotti una legislazione *ad hoc* per il tracciamento dei cittadini tramite *app*. La decisione è stata resa pubblica il 26 aprile 2020, a seguito dell'intervento da parte di una commissione parlamentare di controllo che ha interrotto l'uso delle tecniche di monitoraggio per imporre le quarantene, evidenziando problemi di *privacy*.

La Corte Suprema ha dichiarato che, *«il controllo prolungato dei cittadini pone evidenti problemi di privacy, soprattutto per quanto concerne la gestione dei dati e la loro conservazione con evidenti problemi di costituzionalità, oltre che di etica»*. Si ravvisa, quindi, un "pericolo evidente" nell'utilizzo di un'arma "straordinaria" che potrebbe avere anche dei "risvolti dannosi"[61]. *«La scelta dello Stato di utilizzare un servizio di sicurezza preventiva per monitorare senza alcun danno chi non lo desidera, senza il consenso, solleva grandi problematiche e deve essere trovata un'alternativa adeguata, compatibile con i principi della privacy»*, ha statuito la Corte Suprema. All'interno della sentenza viene anche sottolineata l'importanza di non creare

prestabilite. Il *geofencing* può essere utilizzato nel campo del *marketing*, della sicurezza e della sorveglianza.

[61] *La decisione della Corte Suprema di Israele, del 26 aprile 2020: l'APP di tracciamento solo con legge*, M. PETA, Il Sole 24 Ore, https://www.diritto24.ilsole24ore.com/art/avvocatoAffari/mercatiImpresa/2020-05-04/la-decisione-corte-suprema-israele-26-aprile-2020-app-tracciamento-solo-legge-160910.php, ultimo accesso l'8 maggio 2020.

precedenti pericolosi che potrebbero "giustificare strumenti straordinari e dannosi" per il popolo israeliano[62].

Definita quale set di un film distopico, **Mosca**, capitale anche per numero di contagiati, ha implementato un sistema di tracciamento totale, efficacemente definito "campo di concentramento digitale" o "*cyber-gulag*". Se si sconfina oltre la zona dove si abita, arriverà un sms di avvertimento. I movimenti vengono pedinati dal telefonino, dai pagamenti con le carte di credito e dalle telecamere di riconoscimento, e ogni volta che si esce di casa bisogna farsi rilasciare un *QR-code* personale dal comune: per tracciare i movimenti dei moscoviti in quarantena è stato messo in atto un "sistema da Grande Fratello". Registrandosi su un sito Web governativo o scaricando un'*app* sul proprio *smartphone*, i cittadini devono dichiarare in anticipo partenza, la destinazione e lo scopo di essa; ricevono quindi un codice *QR* che può essere controllato dalle autorità. Tutto ciò allo scopo di garantire l'autodisciplina dei cittadini durante il blocco. In Russia, dove da sempre Putin proclama il sovranismo digitale, le uscite sono, dunque, autorizzate tramite un *QR-code* generato da siti governativi e chi non ha uno *smartphone* lo può affittare con l'*app* già preinstallata.

Ma il vero problema è, ovviamente, la democrazia, che in Russia scarseggiava già prima dell'epidemia. Un tracciamento totale, che coinvolge in un ruolo improprio anche aziende private come operatori telefonici e banche, permetterebbe di bloccare qualsiasi attività sgradita alle autorità, di spiare legalmente gli oppositori e i dissidenti, e anche di utilizzare il pretesto della violazione della quarantena per incarcerare i personaggi scomodi. Molti dissidenti temono anche che, una volta

[62] *Tracciamento Covid-19 in Israele. Il programma dello Shin Bet scadrà il 26 maggio*, P. CASTELLANO, Bet Magazine Mosaico, https://www.mosaico-cem.it/attualita-e-news/israele/tracciamento-shin-bet-israele, ultimo accesso l'8 maggio 2020.

ISSN 2531-6931

finita l'emergenza, le telecamere non si spegneranno e il Grande Fratello diventerà permanente[63].

Roskomsvoboda, una organizzazione non governativa che controlla la libertà di *Internet* in Russia, ha definito il nuovo strumento parte di "*una corsa alla sorveglianza*" e che tale sistema di sorveglianza sia stato sviluppato molto prima della pandemia, sebbene l'irrompere del virus abbia dato maggiore impulso allo sviluppo di tale tecnologia per controllare i movimenti e la comunicazione dei cittadini.

§VIII. **Conclusioni**

La gravissima emergenza che il Paese sta affrontando ha imposto l'adozione – con norme di vario rango – di misure limitative di molti diritti costituzionali, necessarie per contenere auspicabilmente il numero dei contagi.

La protezione dei dati personali – fondamentale diritto "di libertà", sancito dalla copiosa normativa di diritto dell'Unione Europea – non poteva fare, naturalmente, eccezione, benché le limitazioni sinora adottate siano nel complesso contenute. Alcune deroghe al regime ordinario di gestione dei dati sono state previste sin dalle primissime ordinanze intervenute pochi giorni dopo la deliberazione dello stato di emergenza, con prevalente riferimento all'ambito di comunicazione dei dati sanitari.

I diritti fondamentali non sono assoluti; non lo è neppure il diritto alla protezione dei dati che, come gli altri, rientra nell'alveo dell'art 52, par. 1 e 3 della Carta dei diritti fondamentali dell'Unione Europea. Tale disposizione, infatti, prevede che possa essere attribuita una specifica

[63] *Quarantena in Russia. Mosca prova a contenere la malattia con il tracciamento totale*, A. ZAFESOVA, Linkiesta, https://www.linkiesta.it/2020/04/coronavirus-russia-putin-mosca/, ultimo accesso l'8 maggio 2020.

preminenza, ricorrendone determinati presupposti – tra cui senz'altro le situazioni emergenziali in ambito sanitario – agli obiettivi di interesse generale, sanciti nell'art. 3 del Trattato sull'Unione europea.

In presenza di un pericolo per la salute dell'insieme degli altri consociati, dunque, l'esigenza eccezionale di tutela della dimensione collettiva della salute può legittimare il sacrificio della libertà dell'individuo e del diritto alla riservatezza dei dati personali, che, non essendo diritti assoluti, devono necessariamente bilanciarsi con altri interessi pubblici. Il diritto alla *privacy* ed alla riservatezza non trova, difatti, una espressa tutela nella Carta costituzionale – se non per via ermeneutica. Dunque, soccombe innanzi alla preminenza del diritto fondamentale della salute della intera collettività, che ha rango costituzionale.

L'emergenza sanitaria in atto ha imposto e imporrà, verosimilmente ancora, sensibili restrizioni dei diritti individuali. È comprensibile e persino doveroso, anche per realizzare – lo ha ben ricordato il Garante della *privacy* Antonello Soro – quell'istanza solidaristica che caratterizza il diritto alla salute, parallelamente alla sua componente individuale di diritto fondamentale della persona. Purché, naturalmente, le limitazioni previste siano necessarie, adeguate, proporzionali all'esigenza di prevenzione, temporalmente limitate al contesto emergenziale e, come prescrive l'art. 52 della Carta di Nizza, non pregiudichino il contenuto essenziale del diritto.

Le tecniche utilizzate al fine di analizzare l'andamento epidemiologico o per ricostruire la catena dei contagi del COVID-19 comportano una delicata opera di bilanciamento tra il diritto alla salute e il diritto alla riservatezza. Se il primo sembra prevalere nell'immediato, non vanno sottovalutati i rischi futuri derivanti dall'utilizzo esteso di tecniche di controllo del singolo.

L'aspetto fondamentale dell'intervento del Comitato europeo per la protezione dei dati ha riguardato la netta considerazione secondo la quale la tutela della salute e la tutela della riservatezza possono coesistere all'interno dell'attuale panorama normativo, senza alcun bisogno di "sospendere la *privacy*". La questione del rapporto tra i due

ISSN 2531-6931

diritti non può porsi nei termini di *trade-off* tra salute e *privacy*, infatti a un più attento esame appare evidente che la questione non può essere articolata in termini alternativi/oppositivi.

Ma allora, come salvaguardare *sia* la tutela dei dati personali *sia* la salute, a fronte di una minaccia pandemica? Certamente, come proposto dal Garante e dalla dottrina costituzionalista, con un approccio ispirato al criterio di gradualità, il quale fornisce una strategia ragionevole per ogni situazione inedita: occorre, anzitutto, testare l'efficacia delle misure meno invasive e quindi incrementarle in caso di *escalation* della situazione eccezionale.

Alla luce delle considerazioni sopra esposte, deve ritenersi ammissibile – e lo ha ritenuto tale il Garante – l'utilizzo delle attività di *contact tracing* per fornire alle autorità sanitarie dati utili per il contenimento del contagio. Tuttavia, devono sempre essere utilizzate tecniche in grado di garantire l'anonimato e, solo qualora ciò non fosse possibile, predisporre un sistema di garanzie adeguate. In ogni caso, gli Stati membri devono agire nel rispetto del principio di proporzionalità, mediante l'impiego di tecniche meno intrusive possibili. La *privacy*, infatti, non è un surplus, un orpello che si possa mettere o togliere a seconda delle stagioni, ma è il fondamento della libertà dell'individuo perché senza di essa non ci sarebbe libertà di pensiero.

Un'ultima questione, che dovrebbe aprire un dibattito non ancora fiorito, ma solo accennato, attiene al riutilizzo, *a posteriori*, del codice sorgente dell'*app* "Immuni" per esigenze diverse di altre pubbliche amministrazioni o soggetti giuridici; ciò in quanto – secondo quanto asserito dal Commissario nel provvedimento di scelta del *partner* – si è in presenza di una "*licenza d'uso aperta, gratuita e perpetua*" che rimanderebbe agli artt. 68 e 69 del Codice dell'Amministrazione Digitale, sull'acquisizione di un programma informatico e sul suo riuso.

«*Le pubbliche amministrazioni* – recita il disposto ex art. 69 c.a.d. – *che siano titolari di soluzioni e programmi informatici realizzati su specifiche indicazioni del*

committente pubblico, hanno l'obbligo di rendere disponibile il relativo codice sorgente, completo della documentazione e rilasciato in repertorio pubblico sotto licenza aperta, in uso gratuito ad altre pubbliche amministrazioni o ai soggetti giuridici che intendano adattarli alle proprie esigenze, salvo motivate ragioni di ordine e sicurezza pubblica, difesa nazionale e consultazioni elettorali».

Si auspica, di certo, a questo proposito, un intervento della dottrina che possa contribuire allo sviluppo di un dibattito necessario.

«Non vi debbe cadere alcuna considerazione né di giusto né d'ingiusto, né di piatoso né di crudele, né di laudabile né d'ignominioso; anzi, posposto ogni altro rispetto, seguire al tutto quel partito che le salvi la vita».

N. Machiavelli, "Discorsi"

BIBLIOGRAFIA

Enciclopedia del Diritto., vol. XXXV, Milano, 1986.

Il diritto di avere diritti, S. RODOTÀ, Laterza, Roma-Bari, 2012.

Il mondo nella rete. Quali i diritti, quali i vincoli, S. RODOTÀ, Laterza, Roma-Bari, 2014.

I nuovi diritti nella giurisprudenza costituzionale, F. MODUGNO, Giappichelli, Torino, 1995.

Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica, G. ZICCARDI, Raffaello Cortina Editore, Milano, 2015.

L'età dei diritti, N. BOBBIO, Einaudi, Torino, 1990.

La società aperta e i suoi nemici. Platone totalitario - vol. I, K. R. POPPER, D. ANTISERI (a cura di), Armando, Roma, 2014.

Le indagini penali. Profili strutturali di una metamorfosi investigativa, S. SIGNORATO, Giappichelli, Torino, 2018.

Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali, S. NIGER, Wolters Kluwer, 2006.

Rivista italiana diritto e procedura penale, 1967.

Tecnologie per il potere. Come usare i social network in politica, G. ZICCARDI, Raffaello Cortina Editore, Milano, 2019.

Technology and Privacy. The New Landscape, P.E. AGREE e M. ROTEMBERG, Mit Press, Cambridge (Mass.) 2001.

The Right to Privacy, S. WARREN, L. D. BRANDEIS, in *Harward Law Review*, 5, 1890.

ISSN 2531-6931

Un dizionario hacker, A. DI CORINTO, Manni, San Cesario di Lecce, 2014.

SITOGRAFIA

Antonello Soro: emergenza Covid-19, le deroghe sul diritto alla privacy non devono diventare un punto di non ritorno, intervento di A. SORO, Garante per la Protezione dei Dati Personali, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9296264.

App coronavirus: perché la Corea non può essere un modello per l'Italia, L. FILIOS, Osservatorio Diritti, https://www.osservatoriodiritti.it/2020/04/02/app-coronavirus-italia-corea/.

Brevi riflessioni su privacy e costituzionalismo al tempo dei big data, L. CALIFANO, in *Federalismi*. https://www.federalismi.it/ApplOpenFilePDF.cfm?eid=438&dpath=editoriale&dfile=EDITORIALE%5F02052017161209%2Epdf&content=Brevi%2Briflessioni%2Bsu%2Bprivacy%2Be%2Bcostituzionalismo%2Bal%2Btempo%2Bdei%2Bbig%2Bdata&content_auth=%3Cb%3ELicia%2BCalifano%3C%2Fb%3E.

Contact tracing vs il coronavirus, dove va l'Europa: le app dei diversi Paesi, M. R. CARBONE, Agenda Digitale, https://www.agendadigitale.eu/sicurezza/privacy/contact-tracing-vs-il-coronavirus-dove-va-leuropa-le-app-dei-diversi-paesi/.

Contrastare la disinformazione, CONSIGLIO DELL'UNIONE EUROPEA, https://www.consilium.europa.eu/it/policies/covid-19-coronavirus-outbreak-and-the-eu-s-response/fighting-disinformation/.

Coronavirus in Russia: guerra al contagio o contagio dell'informazione?, E. TAFURO AMBROSETTI, ISPI, https://www.ispionline.it/it/pubblicazione/coronavirus-russia-guerra-al-contagio-o-allinformazione-25456.

COVID-19 e norme sul trattamento dei dati sanitari: il GDPR e il modello coreano, V. COLAROCCO, 4C Legal, https://www.4clegal.com/hot-topic/covid-19-norme-trattamento-dati-sanitari-gdpr-modello-coreano#_ftn1.

Covid-19, tra diritto alla salute e tutela della privacy: la scelta che l'Italia deve fare, B. CALDERINI, Agenda Digitale, https://www.agendadigitale.eu/sicurezza/privacy/covid-19-il-difficile-equilibrio-tra-diritto-alla-salute-e-tutela-della-privacy/.

Glossario Intelligence. Il linguaggio degli Organismi informativi, SISTEMA DI INFORMAZIONE PER LA SICUREZZA DELLA REPUBBLICA, 2019.

Immuni, cos'è e come funziona l'app italiana coronavirus, R. BERTI, Agenda Digitale, https://www.agendadigitale.eu/cultura-digitale/immuni-come-funziona-lapp-italiana-contro-il-coronavirus/.

Immuni, il giudizio di esperti: "Con sovranità digitale? Se non obbligatoria non serve a nulla. È open source?", L. GAROFALO, Key4Biz, https://www.key4biz.it/immuni-il-giudizio-di-esperti-con-sovranita-digitale-se-non-obbligatoria-non-serve-a-nulla-e-open-o-no-e-le-vulnerabilita-del-bluetooth/300883/.

I quattro nemici (quasi) invisibili nella prima pandemia dell'era della società dei dati, P. DI SALVO, S. MILAN, Il Manifesto, https://ilmanifesto.it/i-quattro-nemici-quasi-invisibili-nella-prima-pandemia-dellera-della-societa-dei-dati/.

La Cina combatte il Coronavirus con l'IA, C. RAMOTTI, IRPA, https://www.irpa.eu/la-cina-combatte-il-coronavirus-con-lia/.

La decisione della Corte Suprema di Israele, del 26 aprile 2020: l'APP di tracciamento solo con legge, M. PETA, Il Sole 24 Ore, https://www.diritto24.ilsole24ore.com/art/avvocatoAffari/mercatiImpresa/2020-05-04/la-decisione-corte-suprema-israele-26-aprile-2020-app-tracciamento-solo-legge-160910.php.

La disinformazione ai tempi del Covid-19? La Cia ricorda i vecchi tempi (attuali) del Kgb, F. BECHIS, in *Formiche*, https://formiche.net/2020/04/disinformazione-tempi-covid19-cia-vecchi-tempi-kgb/

La pandemia immateriale. Gli effetti del Covid-19 tra social asintomatici e comunicazione istituzionale, M. CALIGIURI, L. GIUNGATO, in SOCIETÀ ITALIANA DI INTELLIGENCE, https://press.socint.org/index.php/home/catalog/book/4.

La tempesta perfetta covid-19, deroghe alla protezione dei dati personali ed esigenze di sorveglianza di massa, G. DELLA MORTE, SIDIBlog, http://www.sidiblog.org/2020/03/30/la-tempesta-perfetta-covid-19-deroghe-alla-protezione-dei-dati-personali-ed-esigenze-di-sorveglianza-di-massa/.

Lotta al coronavirus, Paese che vai privacy che trovi: i diversi approcci (Europa, Cina, Corea, Israele), N. MONTE, G. VACIAGO, Agenda Digitale, https://www.agendadigitale.eu/sicurezza/privacy/lotta-al-coronavirus-paese-che-vai-privacy-che-trovi-i-diversi-approcci-europa-cina-corea-israele/.

Luci e ombre sulla procedura di selezione di "Immuni", l'app del governo di tracciamento del contagio da Covid-19, P. CLARIZIA, E. SCHNEIDER, IRPA, https://www.irpa.eu/luci-e-ombre-sulla-procedura-di-selezione-di-immuni-lapp-del-governo-di-tracciamento-del-contagio-da-covid-19/.

Nel ginepraio delle app di tracciabilità, S. DOMINIONI, ISPI, https://www.ispionline.it/it/pubblicazione/nel-ginepraio-delle-app-di-tracciabilita25873?fbclid=IwAR2XjZqO9xw2BUA7FmGGz9wGssMaQLAhkMHtQpRtvCZBCzEdyPmJG3vB_Co.

Perché l'emergenza Covid-19 non implica la sospensione della privacy, R. ZALLONE, DirittoPrivacy.it, https://dirittoprivacy.it/perche-lemergenza-covid-19-non-implica-la-sospensione-della-privacy/

Privacy: diritto fondamentale oppure no, FROSINI T. F., in *Federalismi*. https://www.federalismi.it/ApplOpenFilePDF.cfm?artid=10767&dpath=document&dfile=06082008154616.pdf&content=Privacy%3A%2Bdiritto%2Bfondamentale%2Boppure%2Bno%2B%2D%2Bstato%2B%2D%2Bdottrina%2B%2D%2B.

Privacy, libertà, dignità. Discorso conclusivo della Conferenza internazionale sulla protezione dei dati, S. RODOTÀ, Garante per la Protezione dei Dati Personali, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1049293.

Prove di bilanciamento tra il diritto alla privacy e il diritto alla salute (pubblica), G. GIAMMATTEI, in *Salvis Juribus*, http://www.salvisjuribus.it/prove-di-bilanciamento-tra-il-diritto-alla-privacy-e-il-diritto-alla-salute-pubblica/

Quarantena in Russia. Mosca prova a contenere la malattia con il tracciamento totale, A. ZAFESOVA, Linkiesta, https://www.linkiesta.it/2020/04/coronavirus-russia-putin-mosca/.

Regolamento Ue 2016/679, ecco tutto ciò che cittadini e PA devono sapere, M. ALOVISIO, Agenda Digitale, https://www.agendadigitale.eu/infrastrutture/nuovo-regolamento-privacy-ue-ecco-tutto-cio-che-cittadini-e-pa-devono-sapere/.

Ricostruzione normativo-giurisprudenziale del diritto alla privacy, V. MARIO, in *Salvis Juribus*. Reperibile all'indirizzo: http://www.salvisjuribus.it/ricostruzione-normativo-giurisprudenziale-del-diritto-alla-privacy/#_ftn1.

Se contro il virus si mobilita il Mossad (e non solo). Analisi del prof. Teti, A. TETI, in *Formiche*, https://formiche.net/2020/04/mossad-coronavirus-israele-intelligence/.

Sorveglianza di massa in Cina, il modello che spaventa l'Occidente, B. CALDERINI, Agenda Digitale, https://www.agendadigitale.eu/sicurezza/privacy/sorveglianza-di-massa-in-cina-cosi-funziona-il-modello-che-spaventa-loccidente/.

ISSN 2531-6931

Tracciamento Covid-19 in Israele. Il programma dello Shin Bet scadrà il 26 maggio, P. CASTELLANO, Bet Magazine Mosaico, https://www.mosaico-cem.it/attualita-e-news/israele/tracciamento-shin-bet-israele.

UN tackles 'infodemic' of misinformation and cybercrime in COVID-19 crisis, The United Nations Department of Global Communications, UNITED NATIONS, https://www.un.org/en/un-coronavirus-communications-team/un-tackling-'infodemic'-misinformation-and-cybercrime-covid-19.

Una rilettura del concetto di sicurezza nell'era digitale e della emergenza normalizzata, G. DE VERGOTTINI, in *Rivista AIC*, 4/2019, p. 2, https://www.rivistaaic.it/it/rivista/ultimi-contributi-pubblicati/giuseppe-de-vergottini/una-rilettura-del-concetto-di-sicurezza-nell-era-digitale-e-della-emergenza-normalizzata.