JUS CIVILE

ALESSANDRO BERNES

Assegnista di ricerca – Università Ca' Foscari di Venezia

REGOLARE LA TECNOLOGIA DI *DIGITAL CONTACT TRACING* ALLA LUCE DELLA PROTEZIONE DEI DATI PERSONALI

SOMMARIO: *1. Tecnologie e diritti al tempo della pandemia. – 2. Le diverse tecniche proposte per le app di contact tracing. – 3. Il percorso regolatorio del tracciamento di prossimità in funzione della protezione dei dati personali. – 4. La ricerca scientifica e… il futuro del digital contact tracing.*

1. – Ha suscitato un intenso dibattito nei Paesi europei, in momenti in cui il dialogo forzatamente corre attraverso la rete [1], l'eventualità, dapprima, e l'adozione, poi, di *mobile apps* che possano aiutare a fronteggiare la pandemia da Covid-19 mediante un rapido "tracciamento dei contatti" (c.d. *digital contact tracing*), intrattenuti da persone trovate in seguito positive al virus.

La scelta di procedere con una soluzione di tal fatta si è resa necessaria, tenuto conto che l'ordinario modo di procedere "analogico", cioè la raccolta di informazioni con la semplice intervista dei contagiati, presenta degli evidenti limiti strutturali – oltre che attinenti alla stessa natura umana, come la memoria – in termini di fattibilità (ad esempio, i contatti avvenuti all'interno di luoghi molto frequentati o sui mezzi di trasporto, per lo più tra sconosciuti) e costi notevoli, soprattutto di tempo, per il personale incaricato [2].

[1] Impossibile riportare qui la moltitudine di importanti contributi scientifici sul tema, pubblicati in lingua italiana e straniera, comunque facilmente accessibili per lo più su riviste dematerializzate, anche interdisciplinari. Limitandosi ad alcune raccolte, si vedano il *Symposium: privacy and contact tracing* contenuto sulla rivista *MediaLaws – Law and Policy of the Media in a Comparative Perspective* (http://www.medialaws.eu/analyses/symposium-privacy-and-contact-tracing/), le numerose riflessioni presenti sulla rivista Diritto, Mercato, Tecnologia (https://www.dimt.it/), nonché quelle apparse su https://www.agendadigitale.eu/ e su https://www.comparativecovidlaw.it/. Ulteriore letteratura verrà opportunamente ripresa e citata nel prosieguo.

[2] L'utilizzo del metodo di tracciamento dei contatti recenti, intercorsi con una persona infetta, è da tem-

Pur avendo alla base soluzioni tecnologiche già praticate nei Paesi dell'Asia orientale (soprattutto Corea del Sud, Cina e Singapore) – invero, molto discusse, per incidere fortemente sui diritti e le libertà fondamentali della persona, tra cui la libera circolazione, la riservatezza e non solo il controllo dell'interessato sul legittimo trattamento dei dati personali [3] –, in Europa [4] si è virato verso l'introduzione di applicazioni per *smartphone* [5] che permettano di (ri-)costruire, in maniera pressoché immediata, la rete di contatti di un soggetto trovato positivo al Covid-19, considerando l'esposizione ravvicinata nonché prolungata per un certo tempo con altre persone – le quali hanno, a loro volta, installato e attivato la medesima *app* [6] – mediante un flusso automatico e continuo di dati tra *device.* Attraverso, poi, un sistema di *alert* e notifiche integrato, diventa relativamente semplice informare i potenziali contagiati circa l'incontro avvenuto, in un dato periodo antecedente, con un soggetto risultato positivo al virus [7].

---

po utilizzato nell'ambito scienza epidemiologica, al fine di ricostruire una mappa di potenziali soggetti che possono aver contratto virus trasmissibili mediante contatto umano, onde fermare la catena di contagio. La caratteristica tradizionale rimane però quella di utilizzare strumenti manuali e non digitali, come ad esempio le interviste, anche telefoniche, operate dal personale sanitario, il quale potrebbe però non essere in grado, materialmente, di contattare tutti i potenziali infetti. Nondimeno, il tracciamento "analogico" presenta, in ogni caso, notevoli implicazioni in relazione al trattamento di dati personali, eventualmente acquisiti e conservati da parte delle autorità sanitarie. In generale, sulla pratica di *contact tracing*, si veda il documento del *ECDC* (*European Centre for Disease Prevention and Control*, *Contact tracing for COVID-19: current evidence, options for scale-up and assessment of resources needed*, 5 maggio 2020, https://www.ecdc.europa.eu/en/publications-data/contact-tracing-covid-19-evidence-scale-up-assessment-resources; ma cfr. anche *WHO*, *Contact tracing in the context of COVID-19*, 10 maggio 2020, https://apps.who.int/iris/rest/bitstreams/1277571/retrieve, nonché Id., *Digital tools for COVID-19 contact tracing. Annex: Contact tracing in the context of COVID-19*, 2 giugno 2020, https://apps.who.int/iris/rest/bitstreams/1279465/retrieve.

[3] In generale, i Paesi richiamati nel testo hanno mostrato incisive restrizioni della libertà personale dell'individuo, dal momento che tendono a tracciare gli spostamenti delle persone, nonché verificare il rispetto dei provvedimenti di "quarantena" cui sono eventualmente sottoposti i soggetti risultati positivi al Covid-19, o ancora condizionare l'accesso a determinati servizi, come quelli di trasporto, ad una *app* che, in forza delle connessioni tra diversi *database*, dimostri che l'individuo non è stato vicino ad un paziente infetto. Per una breve sintesi delle esperienze menzionate, G. ZUNINO, *Coronavirus, app e sistemi per tracciare i positivi: come funzionano (nel mondo, in Italia)*, in *agendadigitale.eu*, 23 aprile 2020.

[4] Alcuni Paesi europei, come il Belgio, hanno sollevato parecchie perplessità e deciso inizialmente di non adottare alcuna *app* di tracciamento digitale. Tuttavia, lo stesso governo belga sembra essere ora tornato sui suoi passi (https://www.brusselstimes.com/news/belgium-all-news/health/129704/belgiums-contact-tracing-app-will-be-ready-this-month/).

[5] Ovvero anche un *laptop*, un *tablet*, un *wearable*.

[6] Tema non secondario rimane l'interoperabilità fra le diverse *app* nazionali nei contatti transfrontalieri: sul punto, si veda EDPB, *Dichiarazione relativa all'impatto sulla protezione dei dati derivante dall'interoperabilità delle applicazioni di tracciamento dei contatti*, 16 giugno 2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statementinteroperabilitycontacttracingapps_it.pdf.

[7] Le riflessioni che seguono ambiscono ad un livello più generale del discorso, anziché focalizzarsi sulla

Sebbene l'utilità di un tale sistema non sia stata finora comprovata né sul piano pratico, né in quello scientifico – data anche la ristrettezza dei tempi di implementazione – l'idea di fondo è che il tracciamento (digitale) dei contatti presenti rilevante efficacia per il gran numero di c.d. pazienti "asintomatici", infetti da Covid-19, i quali, non manifestando alcuna sintomatologia, potrebbero continuare ad avere interazioni con una moltitudine di persone, diffondendo così il contagio [8]. In altri termini, lo strumento tecnologico rappresenta una delle possibili alternative volte a limitare, per quanto possibile, la diffusione della pandemia, monitorando la propagazione del virus e allertando le persone che vi sono state esposte [9]. L'impatto sulla sfera giuridica della persona, in linea di principio, si mostra proporzionato, dal momento che, almeno nella prospettiva europea, non si intendono controllare i movimenti della popolazione, inferire misure di confinamento ovvero agevolare la prova di immunità dal virus, bensì la volontà è quella di permettere di adempiere più facilmente, attraverso la tecnologia, ad un dovere di solidarietà sociale.

La questione del tracciamento automatizzato dei contatti, dunque, prende avvio in un contesto specifico, quello cioè di reazione alla pandemia da Covid-19, richiamante lo "stato d'eccezione" tipico delle situazioni di grave emergenza, laddove particolari misure possono contribuire a salvare delle altre vite umane [10]. Senonché debbono essere, in concreto, sempre contemperati ragionevolmente interessi di rango "costituzionale", come la

---

sola esperienza italiana della *app* nazionale di *contact tracing*, denominata "Immuni" (per approfondire: https://github.com/immuni-app). Per una lista comunque esaustiva delle applicazioni nazionali di tracciamento digitale dei contatti adottate dai diversi Paesi https://lsts.research.vub.be/en/contact-tracing-apps (aggiornamento: settembre 2020).

[8] Sul punto, L. FERRETTI, C. WYMANT, M. KENDALL, L. ZHAO, A. NURTAY, L. ABELER-DÖRNER, M. PARKER, D. BONSALL, C. FRASER, *Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing*, *Science*, 8 maggio 2020, https://science.sciencemag.org/content/368/6491/eabb6936/tab-pdf. I modelli previsionali dicono comunque che un veloce tracciamento dei contatti, di concerto ad una rapida attività di *testing* dei positivi, potrebbe arrivare fino a quasi a ridurre la diffusione della pandemia da Covid-19: così J. ABELER, M. BACKER, U. BUERMEYER, H. ZILLESSEN, *COVID-19 Contact Tracing and Data Protection Can Go Together*, in *JMIR mHealth and uHealth*, 2020, vol. 8, iss. 4, https://mhealth.jmir.org/2020/4/e19359/.

[9] Cfr. G. Comandé, *Non sparate sulla app di tracing e fidiamoci del GDPR: ecco perché*, in *agendadigitale.eu*, 28 aprile 2020. In chiave sinergica, pare necessario che l'apparato statale e, in ogni caso, le autorità sanitarie si mettano nelle condizioni – anche economiche – di avere un sistema organizzativo adeguato, il quale fornisca delle chiare e precise indicazioni operative, ad esempio, al soggetto che riceve la notifica: potrebbe essere la prescrizione almeno dell'auto-isolamento fiduciario ovvero di un *test* di positività al virus ("tampone" o sierologico che sia).

[10] Nel senso che la sorveglianza di massa, all'epoca della pandemia, sia una delle componenti che maggiormente caratterizzano la sanità pubblica, GRUPPO DI LAVORO BIOETICA COVID-19, *Sorveglianza territoriale e tutela della salute pubblica: alcuni aspetti etico-giuridici*, Rapporto ISS COVID-19, n. 34/2020 25 maggio 2020, https://www.epicentro.iss.it/coronavirus/pdf/rapporto-covid-19-34-2020.pdf, p. 1.

salute (individuale) e la sanità (pubblica), e gli altri diritti e libertà fondamentali dell'individuo (circolazione, organizzazione, iniziativa economica, riservatezza, e così via) [11].

L'uso più intenso delle tecnologie, sia affermate che nuove, conduce alla crescita esponenziale di informazioni relative agli individui, circolanti nella "data-sfera" [12], richiedendo perciò una maggiore attenzione al controllo di quest'ultima, in una prospettiva di tutela della persona [13]. Così il *digital contact tracing* si inserisce in questo ampio tema trasversale, sempre più di frequente posto dinanzi all'attenzione del giurista: come ci si può servire della tecnologia per perseguire interessi attinenti al benessere dell'uomo, preservando e garantendo, allo stesso tempo, la sua identità [14]. Quando, poi, lo strumento tecnologico permette, in modo particolare, l'elaborazione automatica di informazioni e queste ultime possono essere ricondotte ad una certa persona fisica, identificata o parimenti identificabile, la protezione dei dati personali costituisce un luogo di confronto privilegiato del diritto con l'informatica [15]. In sostanza, l'esempio delle *app* di tracciamento, da un lato, si mostra come un momento essenziale per trovare una soluzione alla pandemia in atto, nell'intento di salvaguardare la collettività; al contempo, determinandosi una più rapida produzione e susseguente circolazione di informazioni, per il tramite

---

[11] Certo, già il contemperare principi e diritti, tutti rilevanti ma in potenziale contrapposizione, non è un compito facile all'interno di qualunque sistema giuridico in una situazione, per così dire, di "normalità"; a questo si aggiunga, ancora, l'"imprevedibilità" di una situazione pandemica e la velocità con cui occorre fornire delle risposte che si mostrino non solo adeguate, ma pure effettive. In relazione all'applicazione dei criteri di proporzionalità e di ragionevolezza anche nel bilanciamento tra principi, alla luce degli interessi che rispecchiano e delle circostanze che vengono in considerazione nel caso concreto, G. PERLINGIERI, *Profili applicativi della ragionevolezza nel diritto civile*, Napoli, 2015, 103 ss.

[12] Sul significato di tale espressione, V. ZENO-ZENCOVICH, *La "Datasfera". Regole giuridiche per il mondo digitale*, L. SCAFFARDI (a cura di), *I "profili" del diritto. Regole, rischi e opportunità nell'era digitale*, Torino, 2018, 99 ss.

[13] Cfr. sul punto S. RODOTÀ, *Tecnologie e diritti*, Bologna, 1995, 41 ss.

[14] Limitandosi allo specifico riferimento al tema qui oggetto di studio, sulla identità personale, insidiata dalle nuove tecnologie dell'informazione, C. CAMARDI – C. TABARRINI, Contact tracing *ed emergenza sanitaria. "Ordinario" e "straordinario" nella disciplina del diritto al controllo dei dati personali*, in *Nuova giur. civ. comm*., Supplemento, 2020, 33.

[15] Afferma R. PANETTA, *Data tracing, modello coreano o cinese? No, serve una via italiana*, in *Corrierecomunicazioni.it*, 27 marzo 2020, https://www.corrierecomunicazioni.it/digital-economy/data-tracing-modello-coreano-o-cinese-no-serve-una-via-italiana/, che «di fronte a simili emergenze possiamo solo affidarci a due consolidate ed abituali strade, quella scientifica e tecnologica, da un lato, e quella istituzionale e giuridica dall'altra (…) Scienza e regole, tecnologia e diritto, possono fare sempre la differenza per il bene dell'uomo solo se pervase da regole etiche degne di questo nome ossia volte a tutelare la dignità degli individui, tutti, nessuno escluso».

di nuove tecnologie, non si possono adombrare le potenziali ricadute sui diritti fondamentali dell'individuo, ivi compresa la tutela dei dati personali [16].

Il nodo principale risiede nel fatto che il trattamento di dati personali nel tracciamento digitale dei contatti, reso possibile proprio grazie all'intermediazione delle tecnologie dell'informazione, sembra facilmente accedere ad una connotazione di "sorveglianza" [17], eseguita in modo sistematico e su vasta scala, in maniera costante e automatizzata, coinvolgendo finanche "dati sensibili" [18].

Certo, in riferimento al diritto alla protezione dei dati personali, deve essere da subito abbandonata una visione prettamente individualistica della situazione giuridica afferente al singolo [19]: il diritto in questione viene costantemente attraversato da altri e diversi interessi, privati o pubblici, che rendono legittime le varie operazioni eseguite con le informazioni personali altrui, volontariamente o perché necessarie alla stregua delle finalità perseguite dal soggetto diverso dall'interessato [20].

La questione allora non attiene tanto all'*an* delle limitazioni dei diritti individuali, specie tenuto conto della natura, dello scopo e del contesto, come la situazione di emergenza sanitaria, nella quale prende avvio una loro – evidente – compressione, ma soprattutto al *quomodo*, cioè alle modalità in cui si estrinsecano, in pratica, gli effetti di siffatte

---

[16] Nondimeno, vi sono tutte una serie di considerazioni politiche, etiche, filosofiche, che si intrecciano con l'implementazione del *contact tracing*, anche se gode senz'altro di una posizione privilegiata il tema/problema della protezione dei dati personali. In argomento, L. FLORIDI, *Mind the App-Considerations on the Ethical Risks of COVID-19 Apps*, *Philosophy and Technology*, 2020, 33 (2), 167 ss.

[17] Cfr. Y. N. HARARI, *The world after coronavirus*, in *Financial Times*, 20 marzo 2020, https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75. Al di là di aneddoti *orwelliani*, antesignana rimane l'opera di S. Rodotà, *Elaboratori elettronici e controllo sociale*, Bologna, 1973. Più di recente, in riferimento alla *data-driven economy* del presente, S. ZUBOFF, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York, 2019.

[18] Per V. CUFFARO, R. D'ORAZIO, *La protezione dei dati personali ai tempi della pandemia*, in *Corr. giur.*, 2020, 735, l'utilizzo di tecniche di elaborazione dei dati rende legittimo il dubbio, e anzi alimenta la comune percezione dell'identificabilità delle persone sempre a portata di mano. Non vanno trascurate, ancora, le conseguenze sociali che compressioni ai diritti fondamentali della persona potrebbero prodursi in un futuro prossimo. Si parla in proposito di "effetti collaterali", i quali potrebbero essere riconducibili, specie una volta cessata l'emergenza virale, al funzionamento tipicamente massivo del *contact tracing*, ancorché volontario, C. CAMARDI, C. TABARRINI, Contact tracing *ed emergenza sanitaria*, cit., 33.

[19] Per tutti, V. RICCIUTO, *Il contratto ed i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali*, in *Riv. dir. civ.*, 2020, 642 ss., nonché R. SENIGAGLIA, *La dimensione patrimoniale del diritto alla protezione dei dati personali*, in *Contr. e impr.*, 2020, 760 ss.

[20] Sul punto, F. BRAVO, *Sul bilanciamento proporzionale dei diritti e delle libertà "fondamentali", tra mercato e persona: nuovi assetti nell'ordinamento europeo?*, in *Contr. e impr.*, 2018, 208 ss.

restrizioni, mediante l'uso dello strumento tecnologico [21]. Ciò si traduce, peraltro, in scelte particolari dal punto di vista "applicativo": nella società dell'informazione, infatti, la realizzazione degli scopi perseguiti assume sempre più spesso i caratteri di una traduzione algoritmica e soprattutto computazionale [22]. Onde evitare l'accettazione supina di ogni nuova tecnologia – nonché della logica binaria che governa i sistemi informatici – pure nel *digital contact tracing* il percorso da seguire domanda il rispetto, in tutti gli stati e le fasi di sua realizzazione, dei principi cardine di necessità e proporzionalità, dal momento che si tratta sempre di contemperare diritti fondamentali della persona [23].

La risposta normativa alla tecnologia non può che essere quella di soffermarsi, in concreto, sulle modalità attraverso le quali dare attuazione a quei principi – che prendono corpo proprio garantendo la legittimità, la finalità e la proporzionalità richiesta al tracciamento dei contatti [24] – che assicurino la migliore protezione dei dati personali. Compito del giurista, inoltre, è quello di fornire indicazioni costanti per l'implementazione pratica dei principi generali applicabili al trattamento dei dati personali – ma non

---

[21] Stando a D. POLETTI, *Il trattamento dei dati inerenti alla salute nell'epoca della pandemia: cronaca dell'emergenza*, in *Persona e mercato*, 2, 2020, 66, il trattamento dei dati personali altrui e la riservatezza delle persona sono messi a dura prova in tempi di emergenza sanitaria, ridotte quasi ad elementi di intralcio alle iniziative di contenimento del virus. Ancora, osserva A. SORO, *Tracciamento contagi coronavirus, ecco i criteri da seguire*, in *agendadigitale.eu*, 29 marzo 2020, che «nonostante la centralità della protezione dati nella vita individuale e collettiva, le sue limitazioni ci appaiono spesso meno percepibili di quelle relative ad altri diritti». Tendenzialmente le persone paiono meno avvezze a sentire come pressante l'invasione dall'esterno della propria sfera "privata", rispetto alla restrizione delle altre libertà fondamentali, riassumibili, per lo più, nella libertà di circolazione. Tant'è che si sono sollevati persino dei problemi di compatibilità costituzionale della *app* di *contact tracing* in relazione all'art. 16 Cost., laddove la limitazione della circolazione è coperta da riserva di legge rinforzata: si vedano le riflessioni di A. CELOTTO, *"Immuni" e la Costituzione*, in *giustiziacivile.com*, 29 aprile 2020, p. 3. Eppure, *privacy* e *data protection* non rappresentano, come si avrà modo di vedere, né un ostacolo, né elementi che devono essere messi da parte o sospensivamente condizionati al pieno raggiungimento di obiettivi di sanità pubblica.

[22] M. HILDEBRANDT, *Privacy as Protection of the Incomputable Self: From Agnostic to Agonistic Machine Learning*, in *Theoretical Inquiries in Law*, vol. 20, 2019, 83 ss.

[23] Del resto, afferma espressamente l'art. 52 della Carta dei diritti fondamentali dell'Unione Europea, che trova eco pure nel *Considerando* § 4, GDPR, secondo il quale: «*[i]l trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità. Il presente regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica*».

[24] Cfr. Art. 5, GDPR.

anche la soluzione "esecutiva" – a tutti coloro (*data scientists*, *engineers*, *designers*, *developers*, etc.) che si trovano a dover ideare, programmare, sviluppare ed aggiornare le diverse *app* mediante le quali si procede con il tracciamento digitale. Il diritto, senza abbandonare la sua logica ordinante, dovrebbe così essere capace di percepire le tendenze, i rischi e finanche anticipare la risoluzione dei problemi che la tecnologia oggi reca con sé [25].

Se quanto detto è vero, vengono ad intrecciarsi la regolamentazione e l'automazione, dove diritto e informatica si trovano legati in un connubio funzionale – normativo, da un lato, e tecnico, dall'altro – con riferimento allo scopo di protezione dei dati personali e, per questa via, di tutela dei diritti e delle libertà fondamentali dell'individuo. Occorre valutare attentamente tutte le possibilità che la tecnica offre alla scienza giuridica, e viceversa: chiunque concorra alla realizzazione di una *app*, dopotutto, dovrebbe essere in grado di intendere quali e quante informazioni siano necessarie non solo per il suo funzionamento pratico, ma anche proporzionate rispetto al fine perseguito, evitando in ogni caso delle scelte che possano mettere in pericolo, anche in futuro, i valori fondanti una società democratica. In fin dei conti, l'intero ciclo di messa a punto di un programma informatico deve tenere a mente la centralità dell'utilizzatore finale nel disegno complessivo: la persona umana.

2. – Una prima questione riguarda le molteplici "sembianze" che, potenzialmente, le *app* di *contact tracing* possono assumere: la scelta dovrebbe essere orientata verso la soluzione che oltre ad essere giustificata e proporzionata quanto alla interferenza con i diritti fondamentali dell'individuo, tra i quali spicca il diritto alla protezione dei dati personali, si dimostri, al contempo, funzionale a raggiungere l'obiettivo perseguito, pertanto sia efficace.

Scartata sin dall'inizio – alla luce di una serie di perplessità di fondo circa la sua ragionevolezza [26] – la possibilità di tracciamento attraverso strumenti di localizzazione spaziale (per esempio, attraverso le informazioni estrapolabili da celle telefoniche, dai

[25] G. MOBILIO, *L'intelligenza artificiale e i rischi di una "disruption" della regolamentazione giuridica*, in *BioLaw Journal – Rivista di BioDiritto*, n. 2/2020, 405.

[26] Ma sul punto A. MAGGI, *Coronavirus, "App Immuni obbligatoria nelle zone a rischio". Intervista di Affaritaliani.it ad Alberto Gambino, Presidente Italian Academy of the Internet Code*, in *Affaritaliani.it*, 22 aprile 2020, https://www.affaritaliani.it/cronache/coronavirus-app-immuni-obbligatoria-nelle-zone-a-rischio-667908.html.

dati relativi alla transazioni commerciali elettroniche o ancora dal *GPS* integrato nei dispositivi), riscontrabile in alcune soluzioni adottate dai Paesi del Sol Levante, l'Europa si è orientata – seguendo anche le notazioni del *European Data Protection Board*[27] – verso una modalità diversa di *tracing*, operante "*a posteriori*", "a ritroso" e solo eventualmente.

In estrema sintesi, i dati raccolti sulla *app* di un soggetto, risultato positivo al Covid-19, permettono di allertare tutti coloro che, a loro volta, abbiano scaricato e attivato la medesima applicazione, i quali in un periodo precedente e temporalmente delimitato fossero entrati all'interno del (corto) raggio d'azione che la collegata tecnologia *Bluetooth-low-energy* rende praticabile[28]. È bene parlare perciò di un tracciamento "di prossimità": non delle posizioni o degli spostamenti delle persone, ma dei contatti dovunque intrattenuti dal soggetto risultato positivo al Covid-19, in quanto funzionale allo scopo di risalire la "catena degli incontri".

Più nel dettaglio, scaricando l'*app* – senza procedere ad alcuna registrazione dell'utente o sottoscrizione di un *account* – viene automaticamente generata una chiave o *ID* univoco, in maniera casuale; questo codice viene poi associato ad altri *Ephemeral ID* crittografici, che hanno la particolarità di cambiare ad intervalli temporali costanti (ad esempio, 10, 15 o 20 minuti). Attraverso la tecnologia *Bluetooth* attiva, oltre all'invio (registrato) dei vari *EphID* prodotti, vengono altresì "captati" e memorizzati dal dispositivo i codici crittografati presenti per un certo periodo nelle immediate vicinanze, generati dalla medesima applicazione installata su altri *device*[29]: l'*app*, pertanto, andrà a collezionare gli *ID* numerici provenienti dai vari dispositivi che si sono man mano incrociati con il *Bluetooth* attivato; chiavi successivamente conservate, peraltro, direttamente sul terminale stesso[30].

---

[27] In realtà, l'uso di dati relativi agli spostamenti delle persone non è stato proprio messo al bando nemmeno dall'EDPB, *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*, 14 aprile 2020, https://edpb.europa.eu/our-work-tools/our-documents/linee-guida/guidelines-042020-use-location-data-and-contact-tracing_en.

[28] Il funzionamento tecnico dell'*app* in questione, come anche la sua configurazione, assai minimale, sarebbe particolarmente semplice. Per ulteriori informazioni, si vedano i documenti richiamati *infra*, nelle note successive.

[29] Uno dei problemi per il quale, ad esempio, la soluzione di tracciamento mediante *Wi-fi* è stata subito accantonata è il consistente drenaggio della carica del dispositivo. Inoltre, la precisione della tecnologia *Bluetooth* è di gran lunga superiore di quella del *GPS* e delle celle telefoniche (1-2 metri).

[30] A ciò si devono sommare, ancora, i *metadati* necessari per far funzionare poi l'algoritmo "a ritroso", individuando la data del contatto, la durata dell'esposizione e la distanza prestabilita, usati per parametrare il rischio di esposizione e ricevere quindi l'*alert*.

Una volta trovato positivo il soggetto possessore dell'*app*, l'alternativa praticabile, in base alla "architettura" sulla quale è basata l'applicazione, appare duplice: l'invio al *server* delle informazioni raccolte potrebbe essere strutturato in maniera centralizzata ovvero decentralizzata, a seconda che l'attività di *matching* tra i potenziali contagiati e il positivo al Codiv-19 sia svolta dall'autorità in *back-office* ovvero avvenga direttamente *on-device*.

Una prima soluzione disponibile è una piattaforma gestita a livello centrale, di regola dall'autorità pubblica (la più nota è *ROBERT: ROBust and privacy-presERving proximity Tracing*, afferente al consorzio *PEPP-PT: Pan-European Privacy-Preserving Proximity Tracing*[31]). Va subito sottolineato che verrebbero inviati i soli *ID* temporanei raccolti "in entrata" (*local proximity list*), dal singolo *device* del contagiato ai *server* dove andrebbero poi "smistati": il compito di informare i contatti intrattenuti dall'utente infetto è, infatti, affidato al gestore del *back-end server* (che potrebbe prevedere, peraltro, l'intervento umano), operando una conversione, attraverso una tabella, tra i codici temporanei e gli *ID* univoci, forniti direttamente dal *server* stesso al tempo della configurazione di ciascuna *app* dopo l'installazione; ciò determina, naturalmente, l'equivalenza – ma non necessariamente l'identificazione[32] – *one user = one person*. La soluzione centralizzata, in fin dei conti, è istituzionalmente vocata a raccogliere molte più informazioni, anche per le ragioni di velocità e accuratezza nel contattare i soggetti che sono stati esposti al virus, pure in maniera indiretta. In sostanza, il sistema centrale procederà a notificare coloro che presentano i codici (univoci) ricavabili indirettamente da quelli temporanei, raccolti dalla applicazione del soggetto positivo al Covid-19; facendo uso, se del caso, di parametri anche in parte diversi rispetto a quelli spazio-temporali utilizzati dall'*app* per la raccolta dei singoli *ID*.

Diversamente, nel sistema al momento più diffuso, quello decentralizzato (per tutti il *DP^3T: Decentralized Privacy-Preserving Proximity Tracing*[33], seguito dal protocollo *Privacy-Preserving Contact Tracing* relativo ad una serie di *API* nate dal consorzio *Google-Apple*, in costante aggiornamento, ove si rende possibile, tra l'altro, per il tramite di apposite procedure, l'interoperabilità tra i differenti sistemi operativi *mobile*[34]) l'au-

---

[31] Per maggiori dettagli, https://github.com/ROBERT-proximity-tracing/documents/blob/master/ROBERT-specification-EN-v1_0.pdf e https://github.com/pepp-pt/pepp-pt-documentation.

[32] Il *ROBERT* non è molto chiaro sul punto, dal momento che dapprima parla di dati anonimi, in riferimento alle sole informazioni raccolte dalla singola *app* e trasferite al *server* centrale; sottolinea poi che i dati dei contatti vengono salvati sul *server* come pseudonimi.

[33] https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf

[34] https://www.apple.com/covid19/contacttracing. C'è da dire che optando per il sistema decentralizzato,

torità centrale – comunque presente, stante la necessità di avere un *server* dove ricevere e ri-trasmettere gli *ID* generati dai singoli dispositivi – si limita a fornire un codice autorizzativo (*one time password*) all'utilizzatore dell'*app*, se risultato positivo al Covid-19, attraverso il quale risulta possibile effettuare l'*upload* in rete delle sole chiavi crittografiche generate e inviate dal proprio *device* [35]. Con una lista – che funziona pressoché da "albo" – contenente gli *ID* dei soggetti risultati positivi al *test*, costantemente aggiornata e scaricata in modo automatico su tutti i dispositivi, è possibile effettuare il *match* con le chiavi già memorizzate dai vari contatti direttamente sul *device*, sì da generare *intra-app* un *alert* nel caso in cui l'algoritmo produca un risultato superiore alla soglia minima prestabilita per il rischio di contagio.

Mantenendo ferme per i modelli descritti le opportune misure di sicurezza informatica (specie per prevenire eventuali attacchi ai *server* [36]), entrambi presentano dei vantaggi e degli svantaggi quando messi a raffronto con la normativa posta a presidio del trattamento dei dati personali. Tuttavia, la scelta della strategia dovrebbe essere giustificata non solo sulla base del criterio di "gradualità" [37] delle misure di *contact tracing* e del principio di minimizzazione dei dati, bensì tenendo adeguatamente conto delle maggiori utilità (e costi) conseguibili attraverso una architettura piuttosto che l'altra rispetto allo scopo perseguito.

Preliminarmente, occorre individuare, in maniera preventiva, le categorie di informazioni realmente necessarie per l'utilizzo dello strumento del *digital contact tracing*, specialmente quando l'*app* può funzionare, almeno in principio, anche soltanto con dati non personali, prescindendo persino da un vero e proprio "trattamento" [38]. Di conseguenza, ci

---

il consorzio *Google-Apple* ha praticamente reso impossibile, di fatto, lo sviluppo di altre soluzioni realmente competitive e compatibili con l'API proposta.

[35] Precisamente, ai singoli dispositivi vengono inviati gli *ID* giornalieri, dai quali è possibile ricavare, tramite un algoritmo definito, i vari *EphID*, così da controllare se sono presenti nella lista di quelli già raccolti.

[36] L'accumulo di grandi quantità di *file*, in un *database* centrale, ad esempio, costituisce un aspetto critico nell'ipotesi di eventuali *data breach* o altri *leaks*, richiedendo uno sforzo considerevole in termini di sicurezza dei dati.

[37] Così si esprime A. SORO, *Audizione informale, in videoconferenza, del Presidente del Garante per la protezione dei dati personali sull'uso delle nuove tecnologie e della rete per contrastare l'emergenza epidemiologica da Coronavirus*, 8 aprile 2020, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9308774.

[38] Così anche la TASK-FORCE COVID-19 (Italia), Sottogruppo di lavoro "Profili giuridici della gestione dei dati connessa all'emergenza", *Relazione tecnico-giuridica sui profili connessi all'eventuale adozione di una soluzione di contact tracing per il contrasto al Covid-19*, https://innovazione.gov.it/assets/docs/SGdL8%20-%20Relazione%20profili%20giuridici%20contact%20tracing.pdf.

si deve chiedere se sia possibile utilizzare informazioni (ragionevolmente [39]) anonime e, in via residuale, degli pseudonimi, che sono comunque considerati alla stregua di dati personali [40]. Ancora, va rammentato che se le finalità per le quali si trattano i dati personali non richiedono (fin dal principio) o non richiedono più l'identificazione dell'interessato, il titolare del trattamento non è obbligato a conservare, acquisire o trattare ulteriori informazioni per identificare l'interessato ai soli fini del rispetto della normativa in materia di protezione dei dati personali (art. 11, GDPR).

Prendendo il modello centralizzato, il nodo più critico riguarda il fatto che le informazioni trattate dall'amministrazione centrale tendono a rendere molto semplice l'identificabilità della persona. In particolare, all'atto di caricamento dei codici ricevuti, comunque effettuato con l'ausilio del personale socio-sanitario, sarebbe possibile incrociare la scheda anagrafica (*rectius*: dati identificativi) del soggetto risultato positivo con l'*ID* numerico di riferimento. È sempre associato, infatti, un codice univoco all'utilizzatore dell'*app* – ciò che permette, a differenza del modello decentralizzato, di sondare altresì i contatti indiretti, quelli cioè di coloro che hanno incrociato il soggetto infettato per primo – il quale però è noto solo dall'autorità pubblica, mai ai terzi: si tratterebbe allora di dato pseudonimo per l'autorità, ma (relativamente [41]) anonimo per tutti gli altri, dal momento che la chiave di codifica sarebbe loro sconosciuta [42]. Forse una garanzia maggiore, basata su una precisa scelta di *accountability*, potrebbe derivare dal ricorso alla categoria dei c.d. "dati de-identificati" (art. 11, GDPR): quando il titolare del trattamento, in ragione

---

[39] EDPB, *Guidelines 04/2020 on the use of location data and contact tracing tools*, cit., 5, parla di tre criteri fondamentali da seguire per stabilire se un dato è anonimo: «(i) singling-out (isolating an individual in a larger group based on the data); (ii) linkability (linking together two records concerning the same individual); and (iii) inference (deducing, with significant probability, unknown information about an individual)»; ma cfr. anche il *Considerando* § 26, GDPR. Tuttavia, come osserva C. IRTI, *Dato personale, dato anonimo e crisi del modello normativo dell'identità*, in *Juscivile*, 2, 2020, 388, se i dati personali possono essere qualificati come "anonimi" solo qualora l'anonimato sia irreversibile, oggi, anche alla luce delle tecnologie, dei modelli algoritmici e della mole enorme di informazioni reperibili nella Rete, non sembra possibile definire un dato veramente "anonimo".

[40] Sottolinea E. PELLECCHIA, *Dati personali, anonimizzati, pseudonimizzati, de-identificati: combinazioni possibili di livelli molteplici di identificabilità nel GDPR*, in *Nuove leggi civ. comm*., 2020, 362, come con la pseudonimizzazione ci si riferisce, in realtà, ad un metodo di trattamento piuttosto che ad una tipologia di dati.

[41] Cfr. CGUE 19 ottobre 2016, causa C-582/14, caso *Breyer*, per la quale le informazioni che consentono di identificare l'interessato non devono, per forza, essere detenute da un unico soggetto, come, ad esempio, nel caso degli indirizzi *IP*. Sul punto, diffusamente, C. IRTI, *Dato personale, dato anonimo e crisi del modello normativo dell'identità*, cit., 388 ss.

[42] In argomento, A. GADOTTI, *Privacy e contact tracing: cosa può andare storto? Ecco i rischi concreti*, in *agendadigitale.eu*, 7 maggio 2020.

della finalità perseguita, non presenta più alcun interesse a conservare (successivamente) gli identificativi che consentono di ricollegare i dati alle persone, si potrebbe andare ad alleggerire la quantità e la qualità di dati in suo possesso e, di conseguenza, gli obblighi ai quali sottostare; solamente dove l'interessato sia in grado di fornire elementi identificativi, la re-identificazione sarà ulteriormente possibile [43].

Ancora, la trasmissione delle chiavi al *server*, da parte del soggetto positivo al *test* del Covid-19, potrebbe essere associata ad un indirizzo *IP*, il quale è pacificamente inteso come dato personale [44]. Forse, qui varrebbe la pena prevedere la fornitura gratuita di una *Virtual Private Network* (VPN) al momento del caricamento *online* delle chiavi collezionate sul dispositivo, per celare l'informazione, o comunque l'utilizzo di un *proxy* per la connessione al *server*, qualora non sia prevista, per impostazione predefinita (*data protection by default*), la non conservazione ovvero la cancellazione immediata del traffico di rete.

Procedere alla identificazione della persona sarebbe possibile, inoltre, attraverso la realizzazione di un grafo sociale (c.d. *social graph*), mettendo in correlazione i singoli *ID* caricati sul *server* con altre informazioni ausiliari eventualmente in possesso (es. *SMS*, *social network*, *GPS*), sì da desumere chi ha visto chi e quando è avvenuto l'incontro [45]. Peraltro, con l'ausilio di una vera e propria rete di "captatori" *Bluetooth* (facili da installare e poco costosi), si sarebbe addirittura in grado di tracciare gli spostamenti degli utenti, in quanto la cronologia dei movimenti giornalieri di ogni individuo, ricavabile in forza della conversione dei molteplici *EphID* nei codici univoci, è sempre unica e distinta per ciascun membro della popolazione [46].

Un ulteriore questione della soluzione centralizzata riguarda aspetti di natura organiz-

---

[43] Per una precisa analisi dell'art. 11, GDPR, E. PELLECCHIA, *Dati personali, anonimizzati, pseudonimizzati, de-identificati*, cit., 367 ss.

[44] Al riguardo, A. POLIMENI, *Immuni, i presupposti perché sia efficace e pro-privacy*, in *agendigitale.eu*, 24 aprile 2020. Per quanto concerne gli indirizzi *IP*, è sufficiente ricordare il Considerando § 30, GDPR, secondo cui *«[l]e persone fisiche possono essere associate a identificativi online prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli indirizzi IP, a marcatori temporanei (cookies) o a identificativi di altro tipo, come i tag di identificazione a radiofrequenza. Tali identificativi possono lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone fisiche e identificarle»*.

[45] Vedi THE DP-3T PROJECT, *Privacy and Security Risk Evaluation of Digital Proximity Tracing Systems*, 21 aprile 2020, https://github.com/DP3T/documents/blob/master/Security%20analysis/Privacy%20and%20Security%20Attacks%20on%20Digital%20Proximity%20Tracing%20Systems.pdf.

[46] In questo senso GADOTTI, *Privacy e contact tracing*, cit. Cfr. anche M. VEALE, *Analysis of the NHSX Contact Tracing App 'Isle of Wight' Data Protection Impact Assessment*, in *LawArXiv Papers*, 9 maggio 2020, 4.

zativa, relativi all'individuazione, in concreto, dei soggetti che possono accedere ai dati contenuti nell'*app*, i quali dovrebbero essere anche gli unici in possesso delle tabelle di decriptazione, onde procedere alla "lettura" delle informazioni raccolte con il *contact tracing*. Quasi paradossalmente, il sentore diffuso è stato però quello di una sfiducia pressoché totale per le *app* gestite, in maniera accentrata, da parte delle strutture sanitarie nazionali, che sono, peraltro, le stesse deputate alla cura delle persone malate.

Diversamente, la strategia prescelta dalla quasi totalità dei Paesi europei, nonché promossa dagli operatori del mercato – in particolare, la *joint venture* creata da Google e Apple – è stata quella di sottolineare il principale vantaggio che il sistema di tracciamento decentralizzato presenta: dal momento che i codici sono generati, conservati e incrociati tra di loro direttamente sul dispositivo, l'autorità pubblica si trova a processare molte meno informazioni, senza venire nemmeno a conoscenza di coloro i quali non abbiano intrattenuto alcuno scambio di codici con soggetti successivamente trovati positivi al Covid-19 [47]. Eppure, forse con una certa incoerenza, non si guarda molto al fatto che vengono collezionati su milioni di *devices* anche gli *ID*, seppur – astrattamente – anonimi, di soggetti infetti, quindi dati relativi alla salute, che ben potrebbero essere captati con intenzioni malevoli [48].

Nella soluzione decentralizzata, il rischio di identificazione, oltre ad essere correlato ai dati del traffico di rete, è relativo proprio alla conservazione degli *ID* sui dispositivi stessi, qualora il *device* stesso sia oggetto di un attacco informatico, di uno "spionaggio" premeditato (c.d. "*paparazzi attack*" [49]) o comunque il codice dell'infetto possa essere associato ad altre informazioni ausiliarie idonee a identificare quest'ultimo. Sul punto

[47] Si ricordi come vengono condivise le sole informazioni relative ai codici generati e inviati dall'utilizzatore, non anche gli *ID* di coloro che sono entrati nel raggio della *app* di tracciamento, rendendo così molto difficile – ma non impossibile – procedere alla re-identificazione dei vari utenti.

[48] Inoltre, a seguito del *match* positivo sul dispositivo dell'utente, nelle *app* basate sul sistema decentralizzato, ad esempio l'*app* nazionale "Immuni", si è prevista altresì la possibilità che l'*app* possa trasmettere, in modo automatico e secondo un modello probabilistico, alcune informazioni al *backend* di "Immuni" che riguardano: la ricezione o meno di una notifica di esposizione al rischio, la data dell'eventuale ultimo contatto stretto con soggetto risultato positivo, la provincia di domicilio, nonché indicatori tecnici relativi al dispositivo dell'utente e all'utilizzo dell'*app*. Sul punto, GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Provvedimento di autorizzazione al trattamento dei dati personali effettuato attraverso il Sistema di allerta Covid-19 – App Immuni*, 1 giugno 2020, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9356568.

[49] In argomento, V. IOVINO, *Contact tracing, la Francia si disallinea: ecco la sua "terza via"*, in *agendadigitale.eu*, 1 giugno 2020, laddove si menziona anche la proposta di protocollo "misto" DESIRE (https://github.com/3rd-ways-for-EU-exposure-notification/project-DESIRE/blob/master/DESIRE-specification-EN-v1_0.pdf).

però va fatta una precisazione importante: qualsiasi sistema di *digital contact tracing* è vulnerabile a un attacco eseguito da un utente sufficientemente esperto che decida, in modo proattivo, di modificare il funzionamento dell'*app*, ad esempio, in modo da registrare l'ora esatta in cui avviene ogni singolo contatto ovvero di (ri-)trasmettere informazioni "false" (come di positività al virus), estendendone il campo di irradiazione spaziale [50].

In virtù del modello prescelto, deve concludersi, pertanto, che non vi è alcuna certezza circa la "non-presenza" di dati personali nel tracciamento digitale di prossimità, in quanto il rischio è connaturato proprio all'elaborazione automatica di informazioni personali [51]. Di qui, la preoccupazione, segnalata in apertura, circa un suo utilizzo eversivo, distorto o comunque non compatibile con le finalità chiaramente delineate al momento del *download* dell'applicazione; sicché si spiega l'intensa attività dei vari attori europei (ad esempio, la Commissione europea, l'*EDPB*, l'*EDPS* e, nell'esperienza italiana, il Garante), volta a individuare le linee direttrici per implementare una strategia di tutela degli interessati già all'atto dell'ideazione del *software*. In ciò, si salda lo stretto rapporto di complementarietà, oggi maggiormente diffuso nell'ambiente digitale, tra scienza giuridica e tecniche dell'informazione [52].

Comunque sia, entrambe le architetture descritte sono compatibili, in astratto, con i principi generali applicabili al trattamento dei dati personali, in particolare con il principio di minimizzazione, se non altro perché il potenziale rischio di identificazione dei soggetti è lasciato, in realtà, a situazioni per lo più patologiche. Non sembra casuale la scelta di non procedere alla creazione di un *account* personale per ciascun utente, di per sé sproporzionato rispetto alle finalità cui è rivolta l'applicazione: del tutto ingiustificata sarebbe, infatti, la collezione di una serie di informazioni per nulla legate ai requisiti-base di funzionamento del sistema che renda possibile il tracciamento di prossimità [53]. C'è da dire però che questa scelta, sebbene correlata al rispetto del principio di minimizzazione, presenta un inconveniente pratico di inefficienza palese: per la medesima persona è pur sempre possibile attivare l'*app* di *contact tracing* su dispositivi diversi ma

[50] Per non parlare dei rischi derivanti dall'estrazione dei dati da un dispositivo rubato o "clonato".

[51] Come affermato anche dai ricercatori del DP^3T nel documento *Privacy and Security Risk Evaluation of Digital Proximity Tracing Systems*, 21 aprile 2020, https://github.com/DP3T/documents/blob/master/Security%20analysis/Privacy%20and%20Security%20Attacks%20on%20Digital%20Proximity%20Tracing%20Systems.pdf , p. 1.

[52] Per un'introduzione al tema, G. SARTOR, *L'informatica giuridica e le tecnologie dell'informazione*[3], Torino, 2016, 81 ss.

[53] Ne è evidente, ancora, il netto rifiuto del ricorso ai *location data*.

sempre ad essa appartenenti, per il tramite di veri e propri *fake accounts*; questi ultimi potrebbero essere utilizzati in contesti diversi, per periodi di tempo limitato, etc., rendendo, di conseguenza, inefficace ma anche socialmente dannosa la collezione delle informazioni dalle persone. Il possibile *trade-off* tra efficienza tecnologica e garanzia dei dati personali, ancora una volta, non è privo di risvolti pratici, particolarmente rilevanti.

3. – Posto che le operazioni di *contact tracing* possono costituire, potenzialmente, un trattamento sistematico e penetrante di dati personali, la scelta tecnica, in pratica adottata, non è mai neutrale quanto all'interferenza sulla sfera giuridica dell'individuo; anzi, il concreto funzionamento della tecnologia può incidere su plurimi aspetti della sua personalità, tra i quali l'identità, la riservatezza, come pure sulla quantità e sulla qualità di dati personali che vengono raccolti, conservati ed successivamente diffusi, pur nell'ottica del minor sacrificio per l'interessato [54].

Mettendo a confronto i diversi modelli ipotizzati, prima, e implementati, poi, con riferimento al tracciamento digitale dei contatti, si è visto come le tecniche dell'informazione richiedano, in maniera non conflittuale bensì complementare, un'attenta considerazione delle questioni giuridiche sottese all'elaborazione automatica di informazioni, al fine di garantire, allo stesso tempo, il funzionamento delle nuove tecnologie compatibilmente con i diritti fondamentali della persona che ne possono venire intaccati [55].

Assumendo che il *digital contact tracing* rappresenti sempre un trattamento dati personali, ancorché pseudonimi (per esempio, le *Temporary Exposure Key* dell'*app* nazionale italiana "Immuni" [56]), un quesito interessante è quello di domandarsi se il rispetto, da parte del titolare del trattamento, dei principi generali applicabili al trattamento, l'ana-

---

[54] Sul punto, non può che richiamarsi S. RODOTÀ, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Roma-Bari, 2014, 37 ss. Per una diversa prospettiva, L. LESSIG, *Code: And Other Laws of Cyberspace*, Version 2.0, New York, 2006, http://codev2.cc/download+remix/Lessig-Codev2.pdf, p. 24 ss., nonché J.R. REIDENBERG, *Lex Informatica: The Formulation of Information Policy Rules through Technology*, in *Texas Law Review*, 76, 1997, 553 ss.

[55] La sinergia fra tecnologia e diritto, come un'alternativa meritevole di essere percorsa accanto alla tipica definizione di precisi modelli comportamentali, è sottolineata da A. MANTELERO, Digital privacy: *tecnologie "conformate" e regole giuridiche*, in *Privacy digitale. Giuristi e informatici a confronto*, F. BERGADANO, A. MANTELERO, G. RUFFO, G. SARTOR, (a cura di), Torino, 2005, 38.

[56] Così la *Valutazione d'impatto sulla protezione dei dati personali presentata dal Ministero della Salute relativa ai trattamenti effettuati nell'ambito del sistema di allerta Covid-19 denominato "Immuni"*, Nota sugli aspetti tecnologici, 3 giugno 2020, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9357972.

lisi dei rischi ragionevolmente prevedibili e l'implementazione dei canoni della c.d. *privacy by design* e *by default*, ivi compresa l'adozione di misure di sicurezza, tecniche e organizzative, possano bastare, astrattamente, per legittimare il tracciamento, oppure l'intervento del legislatore sia da considerarsi, in tale situazione, dirimente. Allo stesso tempo, ci si deve chiedere se individuare le precise modalità tecniche di funzionamento delle *app*, sempre in relazione al trattamento dei dati personali, sia una compito lasciato ai soli assetti normativi, ovvero sia richiesto, mettendo assieme vincoli giuridici e informatici, l'intervento di ulteriori elementi, all'interno del medesimo processo di definizione di una nuova tecnologia.

Il tema della base giuridica, ovvero del presupposto di liceità (*rectius*: legittimità [57]) del trattamento, sul quale fondare le operazioni compiute con le informazioni ricavabili dalle *app* di tracciamento, se riconducibili a persone fisiche identificabili, si pone come un momento preliminare dell'indagine. La volontarietà, da più parti affermata, circa l'utilizzo dell'applicazione [58] – onde evitare, oltremodo, la violazione dei principi di uguaglianza e di non discriminazione, in ragione del noto fenomeno del *digital divide* – non significa che il trattamento debba basarsi senz'altro sul consenso, ipotesi comunque (astrattamente) possibile. Eppure, la manifestazione di volontà dell'interessato si mostra difficilmente coniugabile con un trattamento posto in essere per la tutela della salute della generalità dei consociati, dal momento che è l'interesse pubblico il motivo per cui si giustifica la raccolta automatizzata di determinate informazioni personali [59]; interesse che, appunto, deve trovare compiuta definizione in una norma di legge dell'Unione Europea o dei singoli Stati membri (art. 6, GDPR) [60]. Quando poi le informazioni trattate

---

[57] In questo preciso senso F. BRAVO, *Il consenso e le altre condizioni di liceità del trattamento di dati personali*, in G. FINOCCHIARO (diretto da), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017, 101 ss.

[58] Per tutti, EDPB, *Guidelines 04/2020 on the use of location data and contact tracing tools*, cit., 4.

[59] *Considerando* § 46, GDPR: «*Alcuni tipi di trattamento dei dati personali possono rispondere sia a rilevanti motivi di interesse pubblico sia agli interessi vitali dell'interessato, per esempio se il trattamento è necessario a fini umanitari, tra l'altro per tenere sotto controllo l'evoluzione di epidemie e la loro diffusione o in casi di emergenze umanitarie, in particolare in casi di catastrofi di origine naturale e umana*». La disciplina di protezione dei dati personali, dunque, contempla già limitazioni necessarie a garantire la salute pubblica, seppur attraverso criteri di proporzionalità, precauzione e temporaneità: così GRUPPO DI LAVORO ISS BIOETICA COVID-19, *Protezione dei dati personali nell'emergenza COVID-19*, Rapporto ISS COVID-19, n. 42/2020, https://www.iss.it/documents/20126/0/Rapporto+ISS+COVID-19+42_2020.pdf/c41c7375-4d41-0cec-e20f-16519b855b43?t=1591865185185, 1.

[60] Prosegue l'art. 6, par. 3, GDPR: «*Tale base giuridica potrebbe contenere disposizioni specifiche per adeguare l'applicazione delle norme del presente regolamento, tra cui: le condizioni generali relative alla liceità del trattamento da parte del titolare del trattamento; le tipologie di dati oggetto del trattamento; gli*

ricadono nell'alveo di dati "sensibili", come appunto quelli sanitari (ad esempio, la conoscenza dello stato di soggetto infetto, al momento della positività al virus), entra in gioco proprio la deroga al divieto di trattare categorie particolari di dati personali: ciò è consentito, in particolare, quando il diritto dell'Unione o dei singoli Paesi, per finalità di sicurezza sanitaria, prevenzione, allerta o controllo di malattie trasmissibili e altre minacce gravi alla salute – motivi di sicuro interesse pubblico – dispongano misure appropriate e specifiche garanzie, al fine di tutelare i diritti e le libertà fondamentali dell'interessato (art. 9, par. 1, lett. *i*, GDPR) [61].

Appurata la necessità di avere, a fondamento dell'intero sistema di *digital conctact tracing*, una base legislativa (per l'Italia, ad esempio, l'art. 6, d.l. 30 aprile 2020, n. 28, conv. in l. 25 giugno 2020, n. 70), l'interrogativo, sopra proposto, emerge con forza crescente [62]: può il diritto, da solo, costituire il solo mezzo idoneo ad individuare le "misure appropriate e specifiche garanzie" che salvaguardino i diritti degli interessati circa un utilizzo sproporzionato dei dati personali che gli strumenti di tracciamento digitale abbisognano?

Posto che la sicurezza dei dati personali costituisce un principio imprescindibile ma funzionale al loro trattamento [63], la risposta deve essere rinvenuta conducendo piuttosto

---

interessati; i soggetti cui possono essere comunicati i dati personali e le finalità per cui sono comunicati; le limitazioni della finalità, i periodi di conservazione e le operazioni e procedure di trattamento, comprese le misure atte a garantire un trattamento lecito e corretto, quali quelle per altre specifiche situazioni di trattamento di cui al capo IX. Il diritto dell'Unione o degli Stati membri persegue un obiettivo di interesse pubblico ed è proporzionato all'obiettivo legittimo perseguito».

[61] Da notare come sia rimasto abbastanza sopito il dibattito circa una eventuale applicazione all'art. 23, GDPR, secondo cui il diritto nazionale o dell'Unione cui è soggetto può limitare, mediante misure legislative, la portata di taluni obblighi e diritti presenti nel Regolamento stesso. Inoltre, stando all'art. 5, Direttiva 2002/58/CE (c.d. "Direttiva *ePrivacy*"), relativa alla vita privata e alle comunicazioni elettroniche – attualmente in fase di revisione e aggiornamento presso le sedi istituzionali europee – sarebbero vietati l'ascolto, la captazione, la memorizzazione e altre forme di intercettazione o di sorveglianza delle comunicazioni, e dei relativi dati sul traffico, ad opera di persone diverse dagli utenti, senza consenso di questi ultimi, eccetto quando ciò venga autorizzato per legge. Tuttavia, non sarebbe impedita l'eventuale memorizzazione tecnica o l'accesso al solo fine di effettuare o facilitare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria a fornire un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente. Così ragionando, la scelta di intervenire giustificando il trattamento dei dati personali per legge, nonché la volontarietà di accesso al servizio di *contact tracing*, appaiono come una soluzione sì "ibrida", ma rispettosa comunque dei dettami normativi di fonte europea.

[62] Va detto però che più di incentrarsi sulle questioni relative alla protezione dei dati personali – se non per i profili e alle condizioni di cui subito si dirà – tutte le normative statali dovrebbero piuttosto focalizzarsi sulle altre attività complementari al tracciamento, predisponendo una organizzazione (di mezzi) mirata, al fine di pervenire, per quanto possibile, ad una pronta reazione ad eventuali nuovi "focolai" (ad esempio, effettuando "tamponi" o test sierologici).

[63] Cfr. A. MANTELERO, *Responsabilità e rischio nel Reg. UE 2016/679*, in *Nuove leggi civ. comm.*, 2017, 155.

un'azione concertata tra la disciplina del trattamento e la strutturazione delle *app* di *tracing* [64]. Ciò che risulta assolutamente necessario implementare, in sostanza, è un apparato di misure tecniche e organizzative preventive, ma anche pro-attive, le quali garantiscano che i diritti dei singoli non vengano oltremodo intaccati, più di quanto strettamente necessario allo scopo specificato [65].

L'attenzione va focalizzata, in particolare, proprio sull'intreccio fra le finalità e le modalità di un trattamento che si dimostri davvero rispettoso dei principi e delle regole applicabili alla protezione dei dati personali [66]. Così, il sistema di *tracing* digitale non dovrebbe essere mai in grado di raccogliere più informazioni di quanto realmente necessario alla resa del servizio fornito di *alert* (come messaggi, numeri di telefono, indirizzi *e-mail*, identificativi del dispositivo), in base al contatto ravvicinato con qualcuno risultato successivamente infetto [67]. D'altronde, non pare ammissibile l'eventualità di un trattamento di dati personali ulteriore, compiuto per altre finalità, cioè per scopi diversi da quelli riconducibili al tracciamento (salvo quanto si dirà in relazione alla ricerca scientifica); sicché i dati raccolti non dovrebbero di per sé permettere successive attività diagnostiche o terapeutiche compiute per il tramite della sola *app* di *tracing*, men che meno il controllo sul rispetto delle misure di auto-isolamento del paziente infetto, finalità, queste, estranee allo scopo precipuo cui l'applicazione di tracciamento è indirizzata [68].

Ora, se la determinazione dell'obiettivo cui è rivolta l'*app* di *tracing* è senz'altro compiuta a monte (per lo più, dal legislatore), mediante un'operazione di contemperamento tra diversi interessi, solamente la tecnica stessa è in grado di confermare, nel processo di definizione del *software* medesimo, quali informazioni si mostrano davvero

---

[64] Come sottolinea R. PANETTA, *Privacy is not dead: it's hiring!*, in ID. (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole di mercato*, Milano, 2019, 28, si parla di un evidente mutamento di prospettiva rispetto allo schema che vede la tecnologia quale elemento logicamente e cronologicamente precedente alla regolamentazione del trattamento dei dati personali.

[65] Equilibrio, molte volte, ostico da realizzare, tenuto conto che le logiche informatiche, anche le più complesse, ragionano pur sempre per valori assoluti (cioè "vero" o "falso"), per lo più rispecchianti l'algebra di Boole.

[66] Come osserva WP-ART. 29, *Opinion 1/2010 on the concepts of "controller" and "processor"*, 16 febbraio 2010, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf, p. 14: «In other words, "means" does not only refer to the technical ways of processing personal data, but also to the "how" of processing, which includes questions like "which data shall be processed", "which third parties shall have access to this data", "when data shall data be deleted", etc.»

[67] Ancorché la tendenza vada, come si è già constatato, nella direzione di informazioni rese (ragionevolmente) anonime.

[68] Cfr. G. RESTA, *La protezione dei dati personali nel diritto dell'emergenza Covid-19*, in *giustiziacivile.com*, 5 maggio 2020, 16.

adeguate, necessarie e proporzionate allo scopo perseguito. Ciò importa, pertanto, una decisione di fondo nello sviluppo dell'*app*, fin dal momento della progettazione (*data protection by design*) e per impostazione predefinita (*data protection by default*), in modo che siano rispettati non solo i principi generali applicabili al trattamento ed integrate le garanzie per espletarlo in maniera legittima, ma previste altresì opportune tecniche per la tutela dei diritti fondamentali delle persone [69]. Così, appunto, il ricorso alla anonimizzazione (come la generalizzazione o la randomizzazione [70]) o alla creazione di dati pseudonimi, o ancora la programmazione minimale, per scelta *standard*, della quantità e della qualità di dati personali raccolti, della portata del trattamento, del periodo di conservazione, etc [71].; una valutazione, questa, particolarmente complessa, spettante per lo più ai titolari del trattamento, che tiene conto non solo delle concrete operazioni compiute con i dati personali, ma in generale «…dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento…» (art. 25, GDPR) [72]. Componenti e variabili, queste, che non fanno altro che enfatizzare il ruolo assunto oggi dal titolare del trattamento nell'adempimento dei suoi obblighi di responsabilizzazione in riferimento alla tutela dell'interessato, riassunti nel principio di *accountability*, da garantire in maniera ponderata, elastica e dinamica [73].

Posta la questione in questi termini, l'aspetto strutturale della *data protection by design*, inscindibilmente legato alla funzione della tecnologia stessa, accompagna la disci-

---

[69] Cfr. *Considerando* § 78, GDPR, ove specificamente si parla di offrire trasparenza per quanto riguarda le funzioni e il trattamento di dati personali e consentire all'interessato di controllare il trattamento dei dati personali. Per la letteratura non giuridica, si rinvia a M. COLESKY, J. C. CAIZA, J. M. DEL ALAMO, J.H. HOEPMAN, Y.S. MARTIN, *A System of Privacy PaŠerns for User Control*, in *Proceedings of SAC 2018: Symposium on Applied Computing*, 2018, https://www.cs.ru.nl/J.H.Hoepman/publications/PatternsforUserControl.pdf. Sul punto, anche infra, par. 4.

[70] V. WP-ART. 29, *Opinion 05/2014 on Anonymisation Techniques*, 10 aprile 2014, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

[71] Così l'art. 25, GDPR, dove non a caso vengono riportate: «(…) sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione (…)». Sulla differenza tecnica fra la *privacy by design* e la *privacy by default*, vedi F. PIZZETTI, *Intelligenza artificiale e protezione dei dati personali*, in ID. (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018, 112 ss.

[72] Per un approfondimento, F. BRAVO, *L'"architettura" del trattamento e la sicurezza dei dati e dei sistemi*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit., 791 ss.

[73] Su quest'ultimo aspetto, G. FINOCCHIARO, *Introduzione al Regolamento Europeo sulla protezione dei dati*, in *Nuove leggi civ. comm.*, 2017, 10 ss.

plina giuridica del sistema di *tracing*, dalla sua ideazione al suo concreto espletamento, in modo tale da far dialogare diritto e tecnica informatica, traducendo pure in termini algoritmici le scelte operate dal punto di vista della protezione dei diritti fondamentali dell'individuo e, nel contempo, constatandone la concreta fattibilità, dal momento prodromico della progettazione dell'*app* sino allo svolgimento delle concrete operazioni in cui si esplica il trattamento. Il dettato normativo, quindi, si apre al coinvolgimento di vari soggetti, aventi competenze diverse, come una sorta di "co-regolazione" da parte di diversi attori [74].

La libertà dell'individuo, dunque, non va scambiata per l'efficienza, mediante una delega cieca all'algoritmo, nella speranza di ottenere una chissà quale soluzione salvifica [75]: l'adozione di una nuova tecnologia richiede sempre, in relazione all'obiettivo prefissato, una valutazione proporzionale in riferimento al suo specifico funzionamento, nonché l'adozione di adeguate cautele per l'identità, la riservatezza, la segretezza delle comunicazioni, e così avanti tutti gli aspetti della persona segnati dall'utilizzo delle tecniche dell'informazione [76]. Eppure, l'analisi sopra effettuata circa il possibile modello di tracciamento, centralizzato o decentralizzato, costituisce l'emersione più evidente dei limiti che la legge sconta nell'assolvere anche al compito di definire, nel dettaglio, le linee tecniche di realizzazione del *software*: la tutela dei diritti fondamentali degli interessati allora non può essere lasciata a mere scelte di fondo, ma richiede una precisa messa a punto tecnica del trattamento medesimo, in modo da prevenire il più possibile eventuali pregiudizi per le persone.

Nondimeno, in continuità con le scelte di progettazione, per il tracciamento di prossimità si pone la strategia di sicurezza dei dati, come la discussione in merito ai meccanismi di memorizzazione delle informazioni, ovvero alle procedure di trasmissione dei dati

---

[74] Cfr. G. MOBILIO, *L'intelligenza artificiale e i rischi di una "disruption" della regolamentazione giuridica*, cit., 414 ss. per una disamina delle possibili relazioni che possono innescarsi tra norme tecniche e norme giuridiche; ma già A. MANTELERO, Digital privacy: *tecnologie "conformate" e regole giuridiche*, cit., 42, laddove si evidenzia che «(…) la suddetta distinzione fra intervento normativo ad opera del legislatore e regolamentazione attraverso il ricorso alle scelte dei privati, fondate sull'autoregolamentazione o sulle dinamiche del mercato, non va interpretata in maniera eccessivamente rigida ed alternativa, essendo immaginabile, ed anzi sovente auspicabile, un'integrazione fra le due fonti, secondo la recente tendenza favorevole a forme di "co-regolazione" di internet».

[75] A. SORO, *Tracciamento contagi coronavirus, ecco i criteri da seguire*, cit.

[76] Per un'analisi particolare dell'approccio richiamato nel testo, M. HILDEBRANDT, *Saved by Design? The Case of Legal Protection by Design*, in *Nanoethics*, 11, 2017, 307 ss., secondo la quale, dal momento che la maggior parte della popolazione non è in grado di capire immediatamente il funzionamento delle tecnologie, queste devono presentate dagli sviluppatori in modo da essere, allo stesso tempo, *testable* e *contestable* da parte di tutti. Sul punto, anche *infra*, par. 4.

al *server*. Pure qui emerge la necessità di prevedere, in concreto, misure tecniche ed organizzative, proporzionate ai rischi sulla sicurezza derivanti dal trattamento di dati personali [77]. Così, la chiave generata dai dispositivi deve presentare elevati *standard* di protezione e resilienza non solo nel momento in cui i dati vengono trasferiti sul *database* centrale (nel modello centralizzato) ovvero sul "*server*-lista" (nel modello decentralizzato), ma anche fin quando sono conservati all'interno dell'*app*. *Standard*, questi, che il legislatore difficilmente può essere in grado di individuare nel dettaglio (come, ad esempio, la crittografia specifica con chiave segreta o l'utilizzo di *hash* [78]), ma che deve per forza delegare alle scelte operazionali dei soggetti "attivi" del trattamento, compreso, naturalmente, il loro sapere tecnico [79].

Parimenti essenziale risulta allora l'organizzazione complessiva sulla quale si fonda il trattamento (*rectius*: tracciamento) stesso, ove in ragione di plurimi elementi e variabili di rischio vengono stabilite le misure tecniche e organizzative adeguate a garantire che per tutta la durata del trattamento, dalla fase prodromica al suo concreto esercizio, esso sia pienamente legittimo [80]. Al fine di ascrivere precisi obblighi e relative responsabilità, è necessario stabilire con assoluta precisione, infatti, chi sono i soggetti che vanno ad assumere la qualifica di titolare del trattamento (ad esempio, autorità pubbliche, per lo più nel campo sanitario); a ciò si aggiungano, ancora, gli eventuali contitolari ovvero responsabili del trattamento, nominati in base a requisiti specifici di affidabilità (anche esterni, *partner* privati, per lo più tecnici, come programmatori, sviluppatori e informatici [81]) e, da ultimo, gli autorizzati/incaricati al trattamento (plausibilmente, medi-

---

[77] Il rimando è all'art. 32, GDPR, dedicato alla sola "sicurezza del trattamento". Non a caso, il legislatore europeo è intervenuto, di recente, con la Direttiva 2016/1148/UE recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (c.d. "Direttiva NIS"), alla quale è stata data attuazione, in Italia, con il d.lgs. 18.5.2018, n. 65. In argomento, F. BRAVO, *L'"architettura" del trattamento e la sicurezza dei dati e dei sistemi*, cit., p. 785 ss., 804 ss.

[78] Al riguardo, G. D'ACQUISTO, M. NALDI, Big data *e* privacy by design. *Anonimizzazione, pseudonimizzazione, sicurezza*, Torino, 2017, 41 ss.

[79] Significativo che proprio il legislatore italiano, , alla luce del nuovo ruolo assunto dal principio di *accountability*, in sede di adeguamento al GDPR (d.lgs. 10.8.2018, n. 108), abbia modificato il d.lgs. 29.7.2003, n. 196 ("Codice della privacy") abrogando l'intero Titolo V – Sicurezza dei dati e dei sistemi della Parte I, nonché l'Allegato B – Disciplinare tecnico in materia di misure minime di sicurezza, per lo più deputati a fornire regole tecniche con riferimento alle misure minime di sicurezza per il trattamento automatizzato di dati personali.

[80] Secondo S. CALZOLAIO, Privacy by design. *Principi, dinamiche, ambizioni del nuovo Reg. Ue 2016/679*, in *Federalismi.it*, n. 24/2017, p. 14, il concetto di *privacy by design* è connaturato proprio al principio di *accountability*, dal momento che arricchisce e specifica i caratteri della progettazione del trattamento.

[81] Cfr. *Considerando* § 78, GDPR: «(…) *In fase di sviluppo, progettazione, selezione e utilizzo di appli-*

ci, operatori socio-sanitari o tecnici amministrativi).

Ora, se la designazione delle autorità pubbliche quali titolari del trattamento, da un lato, non può che spettare al legislatore, almeno nella soluzione delle *app* di tracciamento nazionale [82], non sempre è così per la nomina degli altri soggetti e finanche per l'organizzazione interna in cui si articolano le strutture amministrative. In casi siffatti, regolamenti, protocolli, circolari interne, ma più in generale codici di condotta (art. 40, GDPR), meccanismi di certificazione (art. 42, GDPR), la figura del DPO (art. 37, GDPR), persino atti di autonomia privata (ad esempio, contratti), possono concorrere all'individuazione della struttura della quale il titolare è a capo, in ossequio alle finalità stabilite. Anche se a tutt'oggi quest'ultimo aspetto non è risultato chiaro nelle *app* nazionali [83], la trasparenza dell'assetto organizzativo, che sta dietro al funzionamento dell'applicazione di tracciamento, si mostra come un elemento fondamentale non solo per garantire la fiducia dei cittadini circa l'utilizzo della medesima, ma anche e soprattutto per individuare coloro che, in concreto, sono tenuti a porre in essere le misure che concretano il generale dovere, continuo, di *accountability*, sino alla effettiva attuazione dei diritti che il GDPR riconosce agli interessati (ad esempio, il diritto di accesso, alla cancellazione, alla rettifica, alla limitazione del trattamento, etc.): attività che non possono certo essere lasciate al solo legislatore.

D'altro canto, essendo piuttosto elevato il rischio derivante dal trattamento sistematico e globale di dati personali, approdo obbligato è stata la c.d. *Data Protection Impact*

---

cazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati. I principi della protezione dei dati fin dalla progettazione e di default dovrebbero essere presi in considerazione anche nell'ambito degli appalti pubblici». Le figure del contitolari del trattamento e dei responsabili potrebbe risolvere, almeno in parte, il fatto che la *privacy by design*, nella prospettiva dell'art. 25, GDPR, come osserva S. CALZOLAIO, Privacy by design, p. 16, appare tutta declinata sul titolare del trattamento, e solo indirettamente, per suo tramite, nei confronti di chi architetta e gestisce i sistemi informatici.

[82] Per l'app italiana "Immuni", il legislatore ha scelto il Ministero della salute come titolare del trattamento.

[83] Vedi, ad esempio, il punto 7 ("Soggetti abilitati ai trattamenti") nell'informativa sull'app "Immuni": https://www.immuni.italia.it/app-pn.html. Da Garante per la protezione dei dati personali, *Provvedimento di autorizzazione al trattamento dei dati personali effettuato attraverso il Sistema di allerta Covid-19 – App Immuni*, cit., si desume che il Ministero della salute si avvale di Sogei S.p.a. e del Ministero dell'economia e delle finanze, limitatamente all'utilizzo del Sistema Tessera Sanitaria, che operano in qualità di responsabili del trattamento, cui vanno aggiunti i soggetti individuati dall'art. 6, co. 1°, d.l. 30.4.2020, n. 28, conv. in l. 25.6.2020, n. 70.

Assessment; operazione, questa, particolarmente delicata e, nella pratica, necessariamente predisposta "a più mani", nonché sottoposta al parere dell'autorità di controllo, secondo le regole della valutazione preventiva d'impatto [84]. Infatti, al tempo della pandemia di Covid-19, proprio i "Garanti" nazionali hanno assunto un ruolo fondamentale di traduzione delle idee astratte in linee-guida concrete [85]: dopotutto, il controllo preventivo di un trattamento che presenti un rischio elevato per gli interessati, in assenza di misure adottate dal titolare del trattamento per attenuarlo, rappresenta un passaggio essenziale del rapporto tra l'uso di nuove tecnologie e la concreta incidenza delle medesime sui diritti e libertà delle persone.

Vieppiù che il GDPR non permette alle autorità di controllo di intervenire solo attraverso una valutazione ipotetica dei rischi connessi al trattamento di dati personali, bensì prevede tutta una serie di strumenti che possano garantire un monitoraggio costante, serio ed effettivo di quello che avverrà dopo, in considerazione dell'evoluzione della situazione reale (tuttora incerta) [86]. La protezione dei dati personali coinvolge l'intero *life-cycle* dell'applicazione, dalla sua ideazione al suo sviluppo, alla fase di *test* a quella di uscita, come pure i *feedback* collegati al suo utilizzo; ciò che rappresenta un aspetto di centrale rilevanza anche al fine di muovere verso il miglioramento di qualsivoglia tecnologia dell'informazione.

Sono rimasti, forse, in disparte i rimedi riconosciuti agli interessati dal trattamento (specie il diritto alla cancellazione [87]), come la possibilità di richiedere l'intervento umano ove siano previste misure completamente automatizzate [88]. In particolare, se il legislatore un domani si esprimesse in proposito, l'esito dell'algoritmo potrebbe coincidere fi-

---

[84] Sulla valutazione d'impatto, si veda A. MANTELERO, *Il nuovo approccio della valutazione del rischio nella sicurezza dei dati. Valutazione d'impatto e consultazione preventiva (artt. 32-39)*, in G. FINOCCHIARO (diretto da), *Il nuovo Regolamento europeo sulla privacy*, cit., 287 ss.

[85] Sul carattere multilivello delle procedure di formazione delle regole sul trattamento dei dati personali, C. CAMARDI, C. TABARRINI, Contact tracing *ed emergenza sanitaria*, cit., 38.

[86] Cfr. in particolare l'art. 58, GDPR.

[87] Al riguardo, GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Provvedimento di autorizzazione al trattamento dei dati personali effettuato attraverso il Sistema di allerta Covid-19 – App Immuni*, cit., secondo cui il diritto di cancellazione è esercitabile direttamente tramite l'*app* per tutte le chiavi temporanee (TEK) e gli identificativi di prossimità (RPI) mediante una funzione appositamente messa a disposizione dal *Framework A/G* volta a interrompere l'utilizzo dell'*app* in qualsiasi momento.

[88] In argomento, E. PELLECCHIA, Privacy, *decisioni automatizzate e algoritmi*, in E. TOSI, *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, 2019, p. 420 ss., nonché L. EDWARDS, M. VEALE, *Enslaving the Algorithm: From a «Right to an Explanation» to a «Right to Better Decisions»?*, in *IEEE Security & Privacy*, 16 (3), 2018, p. 46 ss.

nanche con una misura restrittiva ad applicazione automatica (ad esempio, l'obbligo di auto-quarantena)[89]. Il che si traduce nel tema delle garanzie applicabili agli interessati: come potranno difendersi da un trattamento che risulti costruito, di base, su una gestione automatizzata dei dati personali? Il diritto dell'individuo di ottenere la revisione ad opera dell'uomo, all'interno di un procedimento decisionale automatizzato comprendente dati personali, espressamente riconosciuto dall'art. 22 GDPR, sembrerebbe testualmente escluso qualora l'esito algoritmico sia autorizzato dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento. Eppure, per il tramite dell'intervento umano, potrebbero essere corrette – già adesso – eventuali distorsioni e inesattezze dei risultati del *contact tracing*, come i c.d. "falsi positivi" e "falsi negativi", oltre a stemperare i limiti che la tecnologia non è, ancora, in grado di superare (ad esempio, la presenza di un muro tra due *dispositivi* con *app* di tracciamento e *Bluetooth* attivo ovvero il contagio conseguente ad un singolo starnuto…).

La protezione dei dati personali si mostra, dunque, come un elemento essenziale per preservare l'essere umano, in quanto tale, dinanzi all'incessante procedere della tecnologia. Nonostante la proclamata *digital neutrality* del GDPR[90], le scelte tecnologiche effettuate, in fondo, non sono mai veramente indifferenti circa le conseguenze che possono prodursi, anche a livello giuridico, sui diritti e le libertà fondamentali dell'individuo[91].

4. – Un ultimo tema riguarda l'obbligo di eliminare i dati raccolti e conservati non soltanto sui *server*, ma anche nei dispositivi stessi, al termine della situazione emergenziale, la quale dovrebbe consistere, auspicabilmente, in una chiara risposta farmacologica, o quanto prima in un vaccino. La necessaria temporaneità del *digital contact tracing* è dai più sottolineata[92]: una volta superata la fase congiunturale provocata dalla pande-

[89] Cfr. però EDPB, *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*, cit., p. 8, secondo cui le indicazioni successive alla individuazione di un contatto a rischio non dovrebbero essere affidate ad un trattamento totalmente automatizzato.

[90] Vedi *Considerando* § 15, GDPR.

[91] Sulla tecnica intesa come nuova "fonte del diritto" – seppure *soft law* – si rimanda a C. PERLINGIERI, *Coronavirus e tracciamento tecnologico: alcune riflessioni sull'applicazione e sui relativi sistemi di interoperabilità dei dispositivi*, in *Actualidad Jurídica Iberoamericana*, 2020, n. 12-*bis*, p. 838.

[92] Lo stesso EDPS, in una nota, propone la definitiva e irreversibile cancellazione dei dati ovvero l'automatica disinstallazione definitiva dell'*app* (https://edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-12020-contact-tracing-mobile_en.). In verità, si avrebbe comunque un fallimento della *app* di tracciamento qualora non si raggiungesse una soglia piuttosto elevata di *down-*

mia, i dati collezionati dovrebbero, stando alla disciplina dettata per la protezione dei dati personali, essere eliminati definitivamente, anonimizzati, o quanto meno de-identificati, in modo tale da rendere non esporre più a rischi le singole persone fisiche [93].

Una questione particolare riguarda le eventuali informazioni, distinte dagli *ID* individuali, che eventualmente potrebbero essere state inserite nell'applicazione e conservate nei *server* per finalità di ricerca scientifica [94]. La stessa documentazione relativa al protocollo *DP^3T* parla di una possibile, ulteriore funzione delle *app* di *tracing*, attraverso la quale l'utilizzatore dell'applicazione potrebbe scegliere di fare *opt-in* e fornire i suoi dati agli epidemiologi [95].

Dal momento che gli scopi qui perseguiti sarebbero ben diversi dal tracciamento di prossimità inteso in senso stretto, occorre vagliare questa possibilità alla luce della disciplina giuridica sulla protezione dei dati personali. Ancora una volta, è la risposta tecnologica, se correttamente instradata, che può venire in soccorso: l'uso ponderato della tecnica può portare alla *compliance* della disciplina posta a presidio dei dati personali, qualora le finalità appaiano quanto mai essenziali, nell'ambito di una attività di ricerca scientifica rivolta proprio a trovare una risposta efficace alla pandemia [96]. Soprattutto in tempi in cui lo studio è incentrato sul dato, e questo può facilmente essere estratto e circolare, fondamentale è non solo custodire, adeguatamente, le informazioni raccolte per metterle a disposizione degli scienziati, ma anche favorirne la diffusione al fine di valorizzare il progresso, elemento cardine per l'incremento delle conoscenze umane [97].

---

load pari al 60% della popolazione: così uno studio dell'Università di Oxford https://www.research.ox.ac.uk/Article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown.

[93] Così anche l'art. 6, comma 6°, D.L. 30.4.2020, n. 28, conv. in l. 25.6.2020, n. 70: «*L'utilizzo dell'applicazione e della piattaforma, nonché ogni trattamento di dati personali effettuato ai sensi al presente articolo sono interrotti alla data di cessazione dello stato di emergenza disposto con delibera del Consiglio dei ministri del 31 gennaio 2020, e comunque non oltre il 31 dicembre 2020, ed entro la medesima data tutti i dati personali trattati devono essere cancellati o resi definitivamente anonimi*».

[94] Questa, ad esempio, la scelta italiana: «*I dati raccolti attraverso l'applicazione di cui al comma 1 non possono essere trattati per finalità diverse da quella di cui al medesimo comma 1, salva la possibilità di utilizzo in forma aggregata o comunque anonima, per soli fini di sanità pubblica, profilassi, statistici o di ricerca scientifica, ai sensi degli articoli 5, paragrafo 1, lettera a) e 9, paragrafo 2, lettere i) e j), del Regolamento (UE) 2016/679*» (art. 6, co. 3°, D.L. 30.4.2020, n. 28).

[95] THE DP^3T PROJECT, *Decentralized Privacy-Preserving Proximity Tracing*, https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf, p. 11.

[96] Cfr. EDPB, *Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak*, 21 aprile 2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf.

[97] Il passaggio dall'approccio teoria-centrico, incentrato sulla prova della plausibilità del risultato finale,

D'altro canto, per quanto riguarda la possibilità di trattamento ulteriore dei dati personali, utilizzati inizialmente per fini diversi, il GDPR ha riconosciuto l'importanza della ricerca, fissando una vera e propria presunzione di compatibilità dei propositi di attività scientifica con le iniziali intenzioni, le quali hanno dato origine alla raccolta dei dati (art. 5, par. 1, lett. *b*): un ulteriore utilizzo a fini scientifici è considerato compatibile, sempreché vengano rispettate tutte le condizioni per avere un trattamento legittimo e siano adottate, in special modo, le opportune misure tecniche ed organizzative, richiamate dalla norma speciale che esorta l'uso attento della minimizzazione dei dati personali nella ricerca, nonché al ricorso alla anonimizzazione – ove possibile senza pregiudicare le caratteristiche intrinseche dell'informazione – o ancora alla psedonimizzazione (art. 89, par. 1, GDPR) [98]. Inoltre, il ruolo dei comitati etici e l'azione delle autorità di controllo appaiono essenziali al fine di garantire l'effettiva possibilità, mediante controlli adeguati, di una successiva divulgazione dei dati raccolti per finalità di ricerca scientifica [99]. Ciò postula altresì una cooperazione internazionale, non solo all'interno del territorio dell'Unione, bensì con trasferimenti di dati relativi alla salute anche al di fuori dei confini europei [100].

Da quanto è emerso, si può affermare chiaramente che l'intreccio tra tecnologia e diritto costituisce, fisiologicamente, un momento ineludibile del dispiegarsi di soluzioni innovative per contrastare la pandemia in atto. In particolare, il dibattito sorto per una concordanza tra *data protection* e uso sapiente delle nuove tecniche dell'informazione, nell'ottica di tutela dei diritti fondamentali della persona, è sicuramente un lascito importante della tragica epoca presente, soprattutto dal punto di vista della consapevolezza dif-

---

a quello dato-centrico, laddove viene incoraggiata la circolazione dei dati già raccolti, è sottolineato da S. LEONELLI, *La ricerca scientifica nell'era dei Big Data*, Milano, 2018, p. 28 ss.

[98] Alle medesime cautele, è possibile altresì la conservazione dei dati personali per una durata superiore a quella prevista dal perseguimento degli scopi inizialmente previsti (art. 5, par. 1, lett. e, GDPR). In tema, sia permesso il rinvio al nostro *La protezione dei dati personali nell'attività di ricerca scientifica*, in *Nuove leggi civ. comm.*, 2020, p. 190 ss.

[99] Quanto all'importanza di una strategia comune di circolazione dei dati epidemiologici raccolti dalle diverse istituzioni, si veda COMM. EU, *Recommendation on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data*, 8 aprile 2020, https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_contact_tracing_4.pdf, p. 9. Del resto, si rende sempre più indispensabile il direzionamento delle informazioni raccolte verso banche dati (aperte) cui gli studiosi possano accedere facilmente, al fine di eseguire tutte le analisi che gli studi epidemiologici richiedono al tempo della Covid-19, anche per un'utilità futura. I proclami della Commissione europea sono sfociati, poi, nel *European COVID-19 Data Platform* (https://www.covid19dataportal.org/).

[100] Cfr. D. POLETTI, *Il trattamento dei dati inerenti alla salute nell'epoca della pandemia*, cit., p. 68.

fusa circa la compenetrazione fra le scienze giuridiche e l'informatica. In sostanza, l'effettività delle misure di protezione dei dati personali non compete solamente alla disciplina giuridica: il *test* di necessità e proporzionalità richiede, nella società dell'informazione, di tenere conto anche delle soluzioni tecniche, presenti e future. Anzi, è proprio «dotandosi di un'architettura giuridica e tecnologica incentrata sul principio del rispetto rigoroso delle regole in materia di tutela dei dati che si può elevare il livello di fiducia nel sistema, rendendolo appunto *trustworthy*» [101].

Per il futuro, dopotutto, momento fondamentale, quanto alla possibilità di diffondere ancora più capillarmente una applicazione di *contact tracing* – condizione necessaria affinché la tecnologia apporti risultati significativi [102] – non sarà soltanto quello di incrementare la presenza di dispositivi *smart* per tutta la popolazione, bensì valorizzare la fiducia dei cittadini, mettendo definitivamente al bando quella che viene per lo più tacciata come la società della sorveglianza o del controllo sociale [103]. Per questo, un fattore determinante per l'affidamento delle persone nell'utilizzo delle *app* di tracciamento è la dimostrazione che verso i cittadini è garantita la protezione dei dati personali, attraverso una architettura chiara e trasparente [104].

---

[101] G. RESTA, *La protezione dei dati personali nel diritto dell'emergenza Covid-19*, cit., p. 17, il quale parla, in fondo, di un sistema garantistico come presupposto fondamentale per l'estrinsecarsi di una vera e propria "donazione" dei dati a scopi solidaristici. Sulla trasparenza come strumento per infondere fiducia ai cittadini anche EDPB, *Guidelines 04/2020 on the use of location data and contact tracing tools*, cit., p. 3, nonché *Joint Statement on Digital Contact Tracing by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe*, https://rm.coe.int/covid19-joint-statement-28-april/16809e3fd7, p. 7, ove si conferma l'evidente necessità di rendere pubblico prima e durante le operazioni di tracciamento come esso realmente funzioni.

[102] Cfr. V. AZZOLINI, *Immuni, perché piace a pochi: ecco gli errori fatti e come migliorare*, in *agendadigitale.eu*, 31 agosto 2020, ove si riscontra che la diffusione della app Immuni risulta bassa rispetto alle attese. A ciò si aggiungono altresì le non chiare indicazioni da seguire alla ricezione della notifica di possibile esposizione al virus, dal momento che l'allertato dovrebbe solamente mettersi in auto-isolamento e contattare il proprio medico di medicina generale, dal momento che il "tampone" non è immediatamente prescritto dall'Azienda sanitaria locale. Come osserva V. AZZOLINI, *Immuni, perché piace a pochi*, cit., «ciò conferma che non c'è alcuna garanzia della terza T della strategia complessiva (*Trace*, *Test*, *Treat*), vale a dire un tampone, e tanto meno che esso sia eseguito tempestivamente o, comunque, entro un tempo certo».

[103] "Siamo preoccupati che nell'effettiva messa in campo dell'applicazione (o delle applicazioni) si possano insinuare interessi che hanno priorità diverse da quella della tutela dei diritti fondamentali dei cittadini e che quindi siano adottate e implementate soluzioni in deroga alla normativa a protezione dei dati": così *Tracciamento dei contatti e democrazia: lettera aperta ai decisori*, https://nexa.polito.it/lettera-aperta-app-COVID19.

[104] COMM. EU, *Orientamenti sulle app a sostegno della lotta alla pandemia di covid-19 relativamente alla protezione dei dati*, 17 aprile 2020, https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52020XC0417(08)&from=EN, p. 4.

Certo, è naturale che il funzionamento tecnico dell'applicazione o il relativo codice sorgente poco interessano alla gran parte della popolazione; ma anche solo sapere che i dettagli relativi alla programmazione e allo sviluppo dell'applicazione sono stati resi e rimarranno pubblicamente accessibili (*open source*), è tale da rendere più trasparente l'operato in favore di tutti i consociati [105].

Nondimeno, positivo è il fatto che le informazioni da fornire obbligatoriamente agli interessati quanto al trattamento dei dati personali sono state effettivamente rese con modalità chiaramente comprensibili dall'utente, attraverso una interfaccia grafica facilmente accessibile (anche mediante immagini, disegni o icone standardizzate), realizzata all'interno della medesima *app* [106]. La semplificazione circa la comprensione del trattamento, attraverso un linguaggio accessibile per l'interessato, rappresenta, dopotutto, un principio cardine della tutela dei dati personali, che può essere raggiunta sin dal "primo contatto" con l'interessato, rendendolo, al contempo, maggiormente consapevole del valore intrinseco delle informazioni a lui riconducibili [107].

La tecnologia, pertanto, deve sempre presentarsi come accessibile, aperta cioè ad un controllo da parte della comunità, in quanto elemento imprescindibile in una società democratica [108]; ciò dovrebbe spingere le persone ad avere una maggiore fiducia nell'*app* da scaricare, rendendola quindi fondamentale, al pari dell'utilizzo dei dispositivi di protezione individuale [109].

Anche per questo motivo, è tanto più apprezzabile l'attenzione che l'Europa ha dimostrato nel provare a delineare una soluzione unica di tracciamento digitale dei contatti per

---

[105] La trasparenza dell'algoritmo, inoltre, potrebbe essere successivamente oggetto di sindacato da parte degli interessati stessi, avvalendosi, probabilmente, del rimedio collettivo di cui all'art. 80, GDPR. Sul punto, diffusamente, M. HILDEBRANDT, *Privacy as Protection of the Incomputable Self*, cit., p. 119. Diversamente, A. POLIMENI, *Immuni, i presupposti perché sia efficace e pro-privacy*, cit., secondo cui un *software* che tratta dati sensibili dovrebbe essere *closed source* per definizione, previa verifica seria e responsabile da parte di chi di dovere. Non dovrebbe essere la *community* a sorvegliare, ma le autorità preposte.

[106] Così ad esempio l'*app* italiana "Immuni".

[107] Interessante notare come la stessa TASK-FORCE COVID-19, *Relazione tecnico-giuridica sui profili connessi all'eventuale adozione di una soluzione di contact tracing per il contrasto al Covid-19*, cit., suggerisce campagne pubblicitarie informate attraverso *alert* dedicati, quali messaggi del tipo "Oggi salvo vite umane, oggi salvo la mia vita, installo …"

[108] Cfr. G. RESTA, *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza,* in *Pol. dir.*, 2019, p. 233, secondo il quale tra tecnologia e desiderabilità sociale, la mediazione giuridica assume un ruolo centrale.

[109] COMM. EU, *Orientamenti sulle app a sostegno della lotta alla pandemia di covid-19 relativamente alla protezione dei dati*, cit., p. 1.

tutti gli Stati membri, di possibile adozione sull'intero territorio dell'Unione [110]; ma non solo, anche il grande interesse dimostrato da *Apple* e *Google*, nel protocollo comune, sembra voler spostare sul terreno globale una "concorrenza al rialzo", mediante una strategia compatibile con i dettami del trattamento di dati personali e, al contempo, maggiormente rispettosa dei diritti e delle libertà fondamentali dell'uomo e soprattutto della sua dignità [111].

L'occasione della pandemia ha reso tutti più accorti sulla necessità di un uso legittimo (ed etico [112]) della tecnologica, nel pieno rispetto dei diritti fondamentali degli individui in una società democratica [113]. Si è parlato senz'altro di tempi poco maturi in ragione della rapidità di operare delle scelte [114]; ma non si può non concordare sul fatto che una simile prova rappresenta oggi una sfida per il futuro, che possa davvero segnare una solu-

---

[110] Si eviterebbero così le autonome iniziative, differenziate da zona a zona che – in quanto spesso scoordinate e poco verificabili – rischiano di indebolire l'efficacia complessiva della strategia di contrasto: così A. SORO, *Audizione informale, in videoconferenza, del Presidente del Garante per la protezione dei dati personali sull'uso delle nuove tecnologie e della rete per contrastare l'emergenza epidemiologica da Coronavirus*, cit., p. 5. Dopotutto, l'eventuale moltiplicazione di modelli – e non delle *app* che saranno certamente diverse – imporrebbe di ripetere valutazione di impatto tante volte quanti fossero i modelli di riferimento e produrrebbe l'effetto di frammentare inutilmente – a fronte di un problema drammaticamente comune – risposte e soluzioni. In questo senso, «per garantire un livello minimo di scambio e trattamento dei dati, come richiesto dal regolamento generale sulla protezione dei dati, gli sviluppatori di applicazioni di tracciamento dei contatti dovranno concordare un protocollo comune e strutture di dati compatibili»: così EDPB, *Dichiarazione relativa all'impatto sulla protezione dei dati derivante dall'interoperabilità delle applicazioni di tracciamento dei contatti*, cit., p. 2.

[111] Una scelta giustificata anche in relazione al profilo dei possibili danni, non da ultimo alla dignità umana, che un trattamento non corretto di dati personali potrebbe determinare. Sul tema, di recente, C. CAMARDI, *Note critiche in tema di danno da illecito trattamento dei dati personali*, in *Jus Civile*, 3, 2020, p. 796, laddove si afferma che la responsabilità del titolare è, ancor prima che per danni, una responsabilità di natura organizzativa, specie quanto alla sicurezza dei dati. Eppure, l'Autrice sottolinea l'ineffettività del rimedio risarcitorio – sempreché il danneggiato riesca a provare il pregiudizio concreto, causalmente collegato all'ostensione del dato personale – contro l'offensività strutturale, massiva e seriale dell'economia digitale sulla persona, la quale non può più essere sistemicamente regolata soltanto in chiave di responsabilità aquiliana, ma richiede altresì il ricorso ad altri strumenti, preventivi e di tipo macroeconomico (come, ad esempio, il modello *antitrust* statunitense).

[112] Nel senso che l'etica può apparire come una soluzione praticabile – ma complementare rispetto al diritto – laddove la norma giuridica, per la sua intrinseca rigidità, non riesce a disciplinare efficacemente. In argomento, B. WAGNER, *Ethics as an Escape from Regulation: From Ethics-Washing to Ethics-Shopping?*, in E. BAYAMLIOĞLU, I. BARALIUC, L. JANSSENS, M. HILDEBRANDT (a cura di), *Being Profiling. Cogitas ergo sum. 10 Years of Profiling the European Citizen*, Amsterdam, 2018.

[113] R. PANETTA, *Data tracing, modello coreano o cinese? No, serve una via italiana*, cit.; ma cfr. anche il tema della "funzione sociale" del diritto alla protezione dei dati personali, sul quale A. RICCI, *La "funzione sociale" del diritto al trattamento dei dati personali*, in *Contr. impr*., 2017, p. 586 ss.

[114] Cfr. D. POLETTI, *Il trattamento dei dati inerenti alla salute nell'epoca della pandemia*, cit., p. 75.

zione efficace nella società dell'informazione, laddove la tecnologia non deve risultare neutrale, ma essere indirizzata proprio al servizio dell'uomo per salvaguardare la vita, minacciata dalla forza irrefrenabile della natura.