Freedom, Security & Justice: European Legal Studies

Rivista quadrimestrale on line
sullo Spazio europeo di libertà, sicurezza e giustizia

2020, n. 3

EDITORIALE SCIENTIFICA
ES

Rivista scientifica on line "Freedom, Security & Justice: European Legal Studies"
www.fsjeurostudies.eu
Editoriale Scientifica, Via San Biagio dei Librai, 39 - Napoli
CODICE ISSN 2532-2079 - Registrazione presso il Tribunale di Nocera Inferiore n° 3 del 3 marzo 2017

Indice-Sommario

2020, n. 3

APPLICAZIONE DI TRACCIAMENTO *IMMUNI* TRA NORMATIVA NAZIONALE E DIRITTO UE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Serena Crespi*

SOMMARIO: 1. L'applicazione di tracciamento *Immuni*, il d.l. 28 del 30 aprile 2020 e la legislazione UE in materia di dati personali: un quadro d'insieme. – 2. La necessità di disporre di un'applicazione di tracciamento. – 3. Lo strumento giuridico sotteso all'adozione di applicazioni di tracciamento. – 4. Le finalità d'uso delle applicazioni di tracciamento e dei dati personali ivi raccolti. – 5. L'uso solo temporaneo delle applicazioni di tracciamento e dei dati personali ivi raccolti. – 6. Il mantenimento del controllo sulle applicazioni di tracciamento e sui dati personali ivi raccolti: volontarietà, uso di *Bluetooth* e conservazione decentrata. – 7. Il tipo di dati personali raccolti con le applicazioni di tracciamento e la durata della loro conservazione. – 8. Conclusioni.

1. L'applicazione di tracciamento *Immuni*, il d.l. 28 del 30 aprile 2020 e la legislazione UE in materia di dati personali: un quadro d'insieme

Il 30 aprile 2020 l'Italia ha adottato il decreto legge (d.l.) 28 – poi convertito nella legge 70 del 25 giugno 2020 – che, all'art. 6 del capo II intitolato "misure urgenti per l'introduzione del sistema di allerta Covid-19", stabilisce le regole e i limiti di funzionamento dell'applicazione di tracciamento italiana *Immuni*, la quale è operativa nel nostro paese dagli inizi di giugno 2020[1]. Sul presupposto che la precoce

Articolo sottoposto a doppio referaggio anonimo.
* Associato di Diritto dell'Unione europea, Università degli Studi di Milano-Bicocca. Indirizzo e-mail: serena.crespi@unimib.it.
[1] Il decreto legge n. 28 del 30 aprile 2020 è pubblicato in GU n. 111 del 30 aprile 2020. Per la legge di conversione, in GU n. 162 del 29 giugno 2020. L'applicazione *Immuni* è in funzione dall'8 giugno 2020, dopo apposita sperimentazione in alcune regioni italiane. Sulla necessità della sperimentazione, v. par. 8 del *Provvedimento di autorizzazione al trattamento dei dati personali effettuato attraverso il Sistema di allerta Covid-19, App Immuni*, adottato dal Garante della *privacy* il 1° giugno 2020 e reperibile sul sito www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9356568. In dottrina, E. CIRONE, *L'app italiana di contact tracing alla prova del GDPR: dall'habeas data al ratchet effect il passo è breve?*, in *SIDIBlog*, 13 maggio 2020; G.M. RUOTOLO, *Alcune osservazioni sulle App di tracciamento dei contatti e dei contagi alla luce del diritto dell'organizzazione mondiale del commercio*, *ibidem*; G. DELLA MORTE, *Quanto Immuni? Luci, ombre e penombre dell'app selezionata dal Governo*

ISSN 2532-2079
DOI: 10.26321/S.CRESPI.02.2020.03

individuazione degli infetti è un fattore essenziale della strategia di contenimento della diffusione del contagio Covid-19, l'applicazione in esame – che ha come funzione principale quella di tracciare i contatti tra individui sulla base dello scambio di segnali tra dispositivi mobili e, per tale via, d'identificare e allertare coloro che si siano accostati inconsapevolmente al virus[2] – si aggiunge così al tradizionale tracciamento manuale svolto attraverso apposite squadre umane, in tal modo facilitandolo ed accelerandolo. Anche a seguito dell'avvento delle moderne tecnologie, quest'ultimo resta in effetti – in Europa ma anche in Asia[3] ove sono state impiegate le prime applicazioni di tracciamento – la via maestra mediante la quale risalire ai soggetti entrati in contatto con i diffusori di Covid-19[4]. L'intervento umano permette, infatti, una valutazione qualitativamente più elevata dei contatti e dunque dell'epidemia – quanto, ad esempio, all'intensità dell'interazione o alle specificità del luogo dell'interazione o ancora quanto all'eventuale uso, anche cumulativo, di misure di protezione – nonché fornisce supporto ai soggetti allertati nella fase di gestione dell'isolamento e della quarantena sia prima sia dopo l'esito del *test* Covid-19, il quale è necessario per determinare la positività al virus[5].

Nonostante la funzione per lo più ancillare delle applicazioni in esame, l'Italia, forse in ragione dell'elevato numero di contagi registrati, è stato tra i primi Stati membri dell'Unione europea a scegliere di utilizzarle e a renderle operative sul proprio territorio nazionale. Sebbene a marzo 2020 ben venti paesi membri avessero già avviato una riflessione sull'uso di questi strumenti in vista della fase di de-confinamento prevista per l'estate 2020, ai primi di giugno 2020 esse erano pienamente attive solo in otto di essi, ossia, oltre che in Italia, in Austria, Bulgaria, Slovacchia, Cipro, Francia, Polonia e

---

italiano, in *Diritti umani e diritto internazionale*, maggio-agosto 2020, n. 2, p. 303 ss.; ID., *La tempesta perfetta. Covid-19, deroghe alla protezione dei dati personali ed esigenze sorveglianza di massa*, 2020, in *SIDIBlog*, 13 maggio 2020; M. S. BONOMI, *L'app Immuni: tra tutela della salute e protezione dei dati personali*, in *Federalismi. Osservatorio di diritto sanitario*, *Paper*, 24 giugno 2020; S. CRESPI, *Applicazioni di tracciamento a tutela della salute e protezione dei dati personali nell'era Covid-19: quale (nuovo) bilanciamento tra diritti?*, in *Eurojus*, 2020, n. 3, p. 218 ss.

[2] Per un'analisi di dettaglio del funzionamento di *Immuni*, R. BERTI, A. LONGO, S. ZANETTI, *Immuni, cos'è e come funziona l'app italiana coronavirus*, 15 maggio 2020, in *Agenda Digitale*, www.agendadigitale.eu.

[3] Le prime applicazioni di tracciamento disponibili sono state quelle di Singapore e della Corea del Sud. Per un'analisi di queste ultime si rinvia a C. GIROT, *Tracer, non pas traquer: «TraceTogether», l'application mobile de lutte contre le Covid-19 de Singapour*, Dalloz-actualité.fr., 16 aprile 2020; A. MEIJERA, C. WILLIAM, R. WEBSTERB, *The COVID-19-crisis and the information polity: An overview of responses and discussions in twenty-one countries from six continents*, in *Information Polity*. 2020, p. 243 ss., spec. p. 259 ss. (Corea del Sud) e p. 261 ss. (Singapore); S. CRESPI, *Applicazioni di tracciamento*, cit., p. 218 ss.; G. DELLA MORTE, *Quanto Immuni? Luci, ombre e penombre dell'app selezionata dal Governo italiano*, cit., spec. pp. 314-315.

[4] In tal senso, il Comitato europeo per la protezione dei dati personali (EDPB), *Sull'uso dei dati di localizzazione e degli strumenti per il tracciamento dei contatti nel contesto dell'emergenza legata al COVID-19 (04/2020)*, https://edpb.europa.eu/our-work-tools/our-documents/linee-guida/guidelines-042020-use-location-data-and-contact-tracing_it.; nonché espressamente l'art. 6, comma 1, d.l. 28 cit. Quanto all'Asia, v. l'esperienza di Singapore riportata nel dettaglio da C. GIROT, *Tracer, non pas traquer* cit.

[5] Così anche L.C. IVERS, D. J WEITZNER, *Can digital contact tracing make up for lost time?*, in *Lancet Public Health*, 16 luglio 2020, p. 1 ss.

Repubblica ceca[6]. A luglio 2020 sono poi state rese operative anche quelle tedesca e danese[7]. Sono invece ancora ad uno stadio, pur se avanzato, di elaborazione, le applicazioni di tracciamento di Belgio, Irlanda, Spagna Paesi Bassi, Finlandia, Estonia, Lituania. Solo sei Stati membri – Grecia, Lussemburgo, Romania, Malta, Slovenia, Svezia e Ungheria – sembrano ancora adesso orientati ad escluderne l'uso[8]. In Svezia in particolare il Governo ha deciso di ritirare la proposta di un'applicazione di controllo dei sintomi Covid-19 a seguito delle perplessità di taluni esperti nazionali quanto all'adeguata tutela dei dati personali ivi raccolti.

Almeno in linea di principio, le indecisioni emerse tra l'altro in Svezia non sono, quantomeno completamente, destituite di fondamento. Nonostante l'importanza degli strumenti tecnologici in esame nel contesto di emergenze sanitarie come quella in corso sia stata rilevata dalla stessa Commissione europea e dal Centro europeo per la prevenzione e il controllo delle malattie[9], applicazioni di controllo dei sintomi e ancora più quelle di tracciamento, essendo fondate sulla raccolta, l'uso e il trasferimento dei dati personali anche sanitari degli individui per ricostruire la mappa epidemiologica del contagio e/o risalire ai soggetti entrati in contatto con individui positivi al Covid-19, comprimono per natura taluni diritti fondamentali (la libertà di circolazione e il diritto d'impresa anche solo in caso di rischio di positività al Covid-19, il diritto d'associazione, di riunione o la libertà di religione in quanto i dati di contatto raccolti potrebbero portare a identificare l'associazione politica o religiosa frequentata da un certo soggetto tracciato e rilevare così le preferenze politiche o le scelte religiose dello

[6] Quanto alla *App. Corona* austriaca, L. LINKOMIES, *Privacy is the hot issue with Covid contact tracing apps in the EU. European responses vary depending on whether a centralised or decentralised contact tracing app is being deployed*, in *Privacy Laws&Business*, giugno 2020, p. 10 ss. Sull'applicazione *VirusSafe* bulgara, https://www.euractiv.com/section/digital/news/covid-19-mobile-app-available-to-governments-for-a-symbolic-euro/. Sull'applicazione cipriota *CovTrace*, https://covid-19.rise.org.cy/RISE_CovTracer_Privacy_Policy_EN.pdf. L'app *StopCovid* francese è stata adottata con *décret* n. 2020-650 del 29 maggio 2020, poi approvato dal Parlamento a giugno 2020, www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000041936881&dateTexte=20200702. Sull'applicazione polacca *ProteGO,* www.natlawreview.com/article/covid-19-poland-launches-official-tracking-app. In Slovacchia è attiva da aprile 2020 l'applicazione di tracciamento *ZostanZdravy*, www.old.korona.gov.sk/en/COVID19-ZostanZdravy.php. Sulla *eRouska* ceca, https://english.radio.cz/mobile-app-erouska-now-available-iphone-users-8101241.

[7] In tal senso*, Report* dell'agenzia europea FRA, *Coronavirus Pandemic in the EU. Fundamental Rights Implications* (*Bulletin* n. 4) pubblicato a luglio 2020 ma relativo al periodo compreso tra l'1 e il 30 giugno 2020, spec. p. 38. Il Report è reperibile sul sito dell'agenzia stessa.

[8] In merito, *Report* dell'agenzia europea FRA, *Coronavirus Pandemic in the EU. Fundamental Rights Implications with a focus on Contact Tracing Apps*, (*Bulletin* n. 2) pubblicato ad aprile 2020 e relativo al periodo compreso tra il 31 marzo e il 30 aprile 2020, spec. p. 48 ss. Il Report è reperibile sul sito dell'agenzia stessa.

[9] Raccomandazione della Commissione europea dell'8 aprile 2020 relativa a un *pacchetto di strumenti comuni dell'Unione per l'uso della tecnologia e dei dati al fine di contrastare la crisi Covid*-19 *e uscirne, in particolare per quanto riguarda le applicazioni mobili e l'uso di dati anonimizzati sulla mobilità, GUUE* L114/7; nonché la Comunicazione della Commissione europea, *Orientamenti sulle app a sostegno della lotta alla pandemia di covid-19 relativamente alla protezione dei dati* del 17 aprile 2020, in GUUE C 124 I/1.

stesso)[10] e, tra questi, quello alla protezione dei dati personali di cui all'art. 8 della Carta dei diritti fondamentali dell'UE. Sebbene per tutelare il diritto parimenti essenziale alla salute pubblica, l'uso tra l'altro nell'Unione europea di applicazioni come quelle in esame richiede allora di rivedere il bilanciamento tra i diritti fondamentali in gioco e, con particolare riferimento alla protezione dei dati, anche di modulare la disciplina sostanziale prevista prima di tutto dal regolamento UE 2016/679 (GDPR)[11] alla luce della pertinente giurisprudenza interpretativa della Corte di giustizia dell'Unione europea[12].

Che invero la compressione del diritto fondamentale di cui all'art. 8 della Carta e della disciplina del GDPR oltre ciò che è normalmente consentito – e dunque l'uso stesso delle applicazioni di tracciamento negli Stati membri – sia possibile quando si tratti di proteggere il diritto alla salute pubblica in caso di epidemie, emerge dallo stesso GDPR e, in particolare, dagli artt. 9 e 23 anche letti alla luce dei cons. 46 e 73. L'art. 9, par. 2, lett. *i)* e il cons. 46 GDPR prevedono che il trattamento di dati anche sensibili (ad es. relativi alla salute) può considerarsi lecito se necessario "per motivi di interesse pubblico…quali la protezione da gravi minacce per la salute a carattere transfrontaliero" o "a fini umanitari, tra l'altro per tenere sotto controllo "l'evoluzione di epidemie e la

[10] In tal senso, *Bulletin* n. 2 dell'agenzia europea FRA cit. e in dottrina L. RICCIARDI, *Alla ricerca di un bilanciamento tra la protezione dei diritti fondamentali nell'ambito dello Spazio di Libertà, Sicurezza e Giustizia e gli interessi nazionali: il Covid-19 alla prova dei fatti*, in questa *Rivista*, 2020, n. 2, p. 250 ss., spec. p. 256 ss., nonché G. ZARRA, *Sulla compatibilità di misure restrittive, adottate in Italia e nella Regione Campania per contenere l'epidemia di COVID-19, con gli articoli 5 e 2 del Protocollo n. 4 CEDU*, in *Diritti umani e diritto internazionale*, maggio-agosto 2020, n. 2, p. 583 ss.

[11] Il GDPR è stato pubblicato in GUUE L 119/1. Per l'analisi delle singole disposizioni del GDPR, KUNER, BYGRAVE, DOCKSEY (ed.), *The EU General Data Protection Regulation (GDPR). A Commentary,* Oxford, 2020. In realtà, la disciplina sostanziale della protezione dei dati personali rilevante nel caso in esame è costituita anche dalla direttiva (c.d. *e-privacy*) 2002/58 del Parlamento europeo e del Consiglio, del 12 luglio 2002, *relativa al trattamento degli stessi nel settore delle comunicazioni elettroniche*, in GUUE L 201/2002. Il presente contributo si concentrerà tuttavia sull'analisi del solo GDPR, il quale rappresenta l'atto principale nella materia in esame.

[12] In tal senso, Corte di giustizia sentenze 8 aprile 2014, *Digital Rights Ireland*, cause C-293/12 e C-594/12, ECLI:EU:C:2014:238; 13 maggio 2014, *Google Spain*, causa C-131/12, ECLI:EU:C:2014:317; 6 ottobre 2015, *Schrems I*, causa C-362/14, ECLI:EU:C:2015:650; 21 dicembre 2016, *Tele2 Severige e Watson*, cause C-203/15 e 698/15, ECLI:EU:C:2016:970, nonché le concl. avv. gen Sanchez-Bordona, 15 gennaio 2020, *La Qauadrature du Net*, cause C-511/18 e 512/18, ECLI:EU:C:2020:6; *Privacy International*, causa C-623/17, ECLI:EU:C:2020:5; *Ordre des barreaux francophones et germanophones*, ECLI:EU:C:2020:7, causa C-520/18. V. anche la recente sentenza della Corte di giustizia 16 luglio 2016, *Data Protection Commissioner c. Facebook Ireland Ltd e Maximillian Schrems* (c.d. *Schrems II*), causa C-311/18, ECLI:EU:C:2020:559. Per un quadro di insieme di tutte le sentt. precit. mi permetto di rinviare a S. CRESPI, *Diritti fondamentali, Corte di giustizia e riforma del sistema UE di protezione dei dati personali*, in *Rivista italiana di diritto pubblico comunitario*, 2015, p. 819 ss.; ID., *Il trasferimento dei dati personali UE in Stati terzi: dall'Approdo sicuro allo Scudo UE/USA per la* privacy, in *Diritto pubblico comparato ed europeo*, 2016, p. 687 ss.; ID., *Sicurezza nazionale e diritti fondamentali alla luce della giurisprudenza UE in materia di tutela dei dati personali*, in *Rivista italiana di diritto pubblico comunitario*, 2017, n. 5, p. 983 ss. Per un'analisi generale sulla pertinente giurisprudenza UE, v. anche G. CAGGIANO, *La Corte di giustizia consolida il ruolo costituzionale nella materia dei dati personali*, in *Studi integrazione eur.*, 2018, p. 9 ss.; F. ROSSI DAL POZZO, *La giurisprudenza della Corte di giustizia sul trattamento dei dati personali*, in *Annali AISDUE*, vol. I, Bari, 2020, p. 71 ss.

loro diffusione"[13]. L'art. 23, par. 1, lett. *e*) e il cons. 73 GDPR stabiliscono poi che il diritto UE o dello Stato membro cui è soggetto il responsabile del trattamento può limitare, mediante misure legislative, la portata di taluni obblighi e diritti GDPR (quelli di cui agli artt. da 12 a 22 e 34) proprio "per salvaguardare importanti obiettivi di interesse pubblico generale UE o di uno Stato membro in materia *di sanità pubblica*"[14].

Tale libertà non è però senza limiti, non potendo le predette disposizioni del GDPR essere considerate un salvacondotto finalizzato a permettere ai Paesi membri, in ragione dell'emergenza sanitaria in corso, l'adozione di qualsiasi tipo di applicazione di tracciamento e/o di normativa nazionale istitutiva delle stesse. É lo stesso art. 9 GDPR a stabilire le condizioni che permettono il trattamento di dati relativi alla salute in deroga al generale divieto di trattamento dei dati sensibili, prevedendo che tale trattamento sia consentito "se necessario per motivi di sanità pubblica" e se fondato su normative che contengono "misure appropriate e specifiche" per tutelare i diritti dell'interessato. Analogamente, l'art. 23 GDPR circoscrive le limitazioni alla disciplina generale GDPR solo a taluni obblighi e diritti – ossia quelli relativi alle modalità per l'esercizio dei diritti dell'interessato di cui agli artt. 13-22 GDPR (art. 12); all'accesso alle informazioni raccolte dal titolare del trattamento (artt. 13-15), alla rettifica (art. 16) e alla cancellazione dei dati raccolti (art. 17), nonché in alcuni casi al diritto di ottenere una limitazione del trattamento degli stessi (art. 18); al diritto alla portabilità dei dati (art. 20), e a quelli di opposizione (art. 21) e di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato (art. 22); all'obbligo del titolare del trattamento di notificare all'interessato in caso di rettifica o cancellazione dei dati o ancora di limitazione del trattamento (art. 19); nonché a quello di comunicare una violazione dei dati personali raccolti (art. 34). *A contrario*, il GDPR resta allora pienamente applicabile in tutte le parti diverse dagli artt. 12-22 e 34 GDPR. Riprendendo poi principi già espressi dalla giurisprudenza UE[15], l'art. 23 GDPR precisa che le limitazioni che la legislazione nazionale può apportare al GDPR per tutelare la salute pubblica "devono rispettare l'essenza dei diritti e delle libertà fondamentali della Carta e della CEDU in una società democratica ed essere necessarie e proporzionate". Gli Stati membri dell'UE – e tra questi l'Italia – che scelgano di dotarsi di strumenti (ad es. l'applicazione di tracciamento *Immuni*) che per natura condizionano il diritto alla protezione dei dati e la disciplina positiva dello stesso contenuta nel GDPR devono, in altri termini, adottare legislazioni interne (art. 6 d.l. 28) nel rispetto dei predetti limiti

[13] Il considerando 46 si riferisce all'art. 6 GDPR che disciplina la liceità del trattamento dei dati. Corsivo aggiunto dall'autore.
[14] Corsivo aggiunto dall'autore.
[15] Così, Corte di giustizia *Digital Rights Ireland* cit. e *Tele2* cit. quanto a misure interne adottate per lottare contro la criminalità; *Schrems I* e *Schrems II* già cit. quanto a misure interne motivate dall'esigenza di garantire la sicurezza nazionale; nonché il parere della Corte di giustizia del 26 luglio 2017 quanto all'accordo PNR tra UE e Canada, ECLI:EU:C:2017:592, parr. 179-180, ove il giudice di Lussemburgo, proprio alla luce dei principi di necessità e proporzionalità, ha confermato la validità dell'art. 3, par. 4, dell'accordo PNR che consente, in circostanze eccezionali e dettagliate, all'autorità canadese competente di trattare i dati PNR se necessario per salvaguardare gli interessi vitali di una persona, in particolare in caso…di rischio grave per la sanità pubblica.

indicati dallo stesso GDPR, i quali sono peraltro in gran parte ispirati ai principi UE di necessità e proporzionalità[16]. Ciò permette di limitare l'intrusività delle applicazioni di tracciamento e ne garantisce la conformità al diritto comune rilevante, evitando di esporre i Paesi membri a procedure di infrazione e rafforzando la fiducia dei cittadini che è alla base del successo di applicazioni ad installazione volontaria, non essendo possibile in sistemi democratici come quello UE (art. 2 TUE) prevedere applicazioni obbligatorie, come invece fatto in Cina, Qatar o Taiwan[17].

Né invero una tesi diversa – che riconosca cioè agli Stati membri una piena libertà d'azione – potrebbe essere sostenuta rivendicando la competenza nazionale in materia di salute, avendo in tale ambito l'Unione europea un potere solo di sostegno e completamento delle iniziative degli Stati membri (artt. 6 e 168 TFUE)[18]. La disciplina GDPR si applica in effetti a ogni trattamento di dati – essa è per così dire orizzontale – e non varia dunque in funzione del tipo e dell'intensità delle competenze UE o nazionali. Inoltre, secondo una giurisprudenza UE ormai costante, neppure ambiti di competenza esclusiva dei Paesi membri – non menzionati cioè nei trattati – sfuggono del tutto al rispetto del diritto comune in situazioni ricadenti nell'ambito di applicazione di quest'ultimo[19], dovendo, anche in tal caso, le legislazioni interne tener conto – e dunque rispettare – le regole UE con le quali le prime entrino in conflitto. Se ciò vale per ambiti di competenza nazionale neppure menzionati nei trattati, questo principio generale si applica allora anche a un ambito come quello in esame (salute) che riconosce all'Unione europea un certo potere (di sostengo e coordinamento delle azioni nazionali). E in effetti

[16] In tal senso anche il Comitato europeo per la protezione dei dati personali (EDPB), *Statement on restrictions on data subject rights in connection to the state of emergency in Member States*, 2 giugno 2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_art_23gdpr_20200602_en.pdf, in particolare parr. 3, 5, 10, 12 e 14. Sull'applicazione del principio di proporzionalità nel settore in esame, C. TRANBERG, *Proportionality and data protection in the case law of the European Court of Justice*, in *Inter. Data Privacy Law*, n. 4, novembre 2011, p. 239 ss. Quanto a quello di necessità, C. COLAPIETRO, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale,* in *Federalismi*, 2018, n. 22, p. 1 ss.

[17] Un po' sorprendentemente, sembrano invece lasciare intendere la possibilità di introdurre anche nella UE applicazioni di tracciamento invasive come quelle cinesi o sudcoreane D. DE FALCO, M.L. MADDALENA, *La politica del tracciamento dei contatti e dei test per covid-19 alla luce delle ultime direttive OMS: nessun ostacolo giuridico impedisce di utilizzare il "modello coreano" anche in Italia*, in *Federalismi. Osservatorio sull'emergenza Covid-19*, *Paper*, 28 marzo 2020, spec. p. 8 ss.

[18] Sulla competenza UE in materia di sanità, v. in generale F. BESTAGNO, *La tutela della salute tra competenze dell'Unione europea e degli Stati membr*i, in *Studi sull'integrazione europea*, 2017, n. 2, p. 317 ss.; B. DE WITTE, *Les competénces exclusives des Ètats members existent-elles?*, in AA.VV, Liber Amicorum *Antonio Tizzano*. *De la Cour CECA à la Cour de l'Union : le long parcours de la justice européenne*, Torino, 2018, p. 306.

[19] Così, *ex multis*, Corte di giustizia, sentenza del 24 novembre 1998, *Bickel e Franz*, causa C-274/96, ECLI:EU:C:1998:563, punto 17 in materia penale; sentenza del 2 ottobre 2003, *Garcia Avello*, causa C-148/02, ECLI:EU:C:2003:539, punto 25 sul nome delle persone; sentenza del 12 luglio 2005, *Schempp*, causa C-403/03, ECLI:EU:C:2005:446, punto 19 in materia di fiscalità diretta; sentenza del 12 settembre 2006, *Spagna c. Regno Unito*, causa C-145/04, ECLI:EU:C:2006:543, punto 78 riguardo al diritto di elettorato alle elezioni del PE; sentenza del 2 marzo 2010, *Rottmann*, causa C-135/08, ECLI:EU:C:2010:104, punto 41 quanto alla cittadinanza di uno Stato membro.

la Corte di giustizia ha previsto l'applicazione di tale principio UE anche nel settore della sanità pubblica[20].

È invece più difficile stabilire se, anche ricorrendo a un'interpretazione per lo più estensiva dei trattati, sarebbe stato possibile ivi individuare una base giuridica per l'adozione di un'applicazione di tracciamento comune. Essendo di fatto queste ultime solo un mezzo a sostengo delle politiche sanitarie nazionali, gli Stati membri, valorizzando la funzione solo tecnica e di coordinamento sottesa agli strumenti in esame, avrebbero potuto tentare di impiegare l'art. 168 TFUE, il quale autorizza per l'appunto all'Unione europea a interventi solo di sostegno e coordinamento. Peraltro, il considerando 25 della decisione 1082/2013 del Parlamento europeo e del Consiglio del 22 ottobre 2013 relativa alle gravi minacce per la salute a carattere transfrontaliero – adottata proprio sulla base dell'art. 168 TFUE – prevede che "il verificarsi di un evento connesso a minacce transfrontaliere gravi per la salute e suscettibile di avere un'incidenza su scala europea" – e dunque in caso di pandemie – "potrebbe imporre agli Stati membri interessati di adottare in modo coordinato particolari misure di controllo…di contatti, al fine di individuare le persone contaminate e quelle esposte al rischio. Tale collaborazione potrebbe richiedere lo scambio di dati personali tramite apposito sistema, tra cui dati sensibili relativi alla salute e informazioni su casi umani di malattia confermati o sospettati, tra gli Stati membri direttamente interessati dalle misure di ricerca di contatti" [21]. L'adozione di un'unica applicazione di tracciamento a livello UE, la quale è proprio uno strumento di controllo dei contatti finalizzato a individuare soggetti infetti o esposti al rischio di contagio mediante lo scambio di dati personali sensibili nel caso di minacce sanitarie a carattere transfrontaliero, avrebbe allora potuto essere intesa come l'attuazione concreta dello scenario delineato al considerando 25 della decisione 1082/2013 oltre i meccanismi ivi già delineati. Inoltre, e seppur usando un'interpretazione particolarmente creativa, il divieto di armonizzare le disposizioni, legislative e regolamentari, interne di cui al par. 5 dell'art. 168 TFUE avrebbe potuto essere considerato rispettato in quanto, fino a pochi mesi fa, nessun ordinamento nazionale disponeva di leggi istitutive di applicazioni di tracciamento, cosicché l'eventuale atto UE non avrebbe di fatto armonizzato alcuna disposizione nazionale[22].

Posto inoltre che, a fronte della (ormai di nuovo, tendenzialmente, piena) libera circolazione delle persone, l'adozione di un'unica applicazione di tracciamento che permettesse di rilevare i contatti anche tra residenti di diversi Paesi membri sarebbe

[20] In tal senso, Corte giustizia, sentenza del 16 maggio 2006, causa C-372/04, *Yvonne Watts c. Bedford Primary Care Trust e Secretary of State for Health*, ECLI:EU:C:2006:325, spec. punto 92; nonché la precedente sentenza della Corte giustizia del 12 luglio 2001, causa C-157/99, *B.S.M. Smits e Stichting Ziekenfonds VGZ, H. T. M. Peerbooms e Stichting CZ Groep Zorgverzekeringen*, ECLI:EU:C:2001:404, spec. punti 44-46.

[21] In GUUE L 293/1 del 5 novembre 2013.

[22] Quella qui proposta è un'interpretazione particolarmente estensiva dell'art. 168 TFUE, la quale è invece totalmente escluse da P. DE PASQUALE, *Le competenze dell'Unione europea in materia di sanità pubblica e la pandemia di Covid-19*, in *Saggi – DPCE online*, 2020, n. 2, p. 2295 ss., spec. pp. 2297-2300, la quale propone invece un'interpretazione lineare della medesima norma.

stata uno strumento più utile al contrasto della pandemia, per natura transfrontaliera, gli Stati membri avrebbero anche potuto cercare di impiegare come base giuridica l'art. 114 TFUE che permette il ravvicinamento delle legislazioni nazionali (quelle istitutive di applicazioni di tracciamento in ogni caso non ancora adottate a livello interno) per raggiungere gli obiettivi UE di cui all'art. 26 TFUE e dunque per la piena realizzazione del mercato interno anche in periodo di pandemia[23].

Le indubbie difficoltà di trovare, quantomeno nella versione attuale dei trattati, una via giuridica adeguata per l'istituzione di un'applicazione di tracciamento UE ha probabilmente motivato gli Stati membri ad adottare nell'ambito in esame iniziative invece solo individuali, in tal modo obbligando la Commissione europea[24] e il Comitato europeo per la protezione dei dati[25] a elaborare meccanismi tecnici e giuridici, al momento ancora in via di adozione, per rendere al più presto almeno interoperative le singole applicazioni di tracciamento nazionali[26].

Al fine di valutare la conformità dell'art. 6 d.l. 28 al GDPR e ai principi di necessità e di proporzionalità – obiettivo del presente contributo – un'utile guida è costituita dalla Comunicazione del 17 aprile 2020 della Commissione europea[27] che, al fine di garantire un approccio coerente in tutta l'Unione, fornisce agli Stati membri e agli sviluppatori di applicazioni di tracciamento una serie di indicazioni pratiche, seppur non vincolanti, circa i requisiti che esse devono possedere per rispettare la pertinente legislazione e giurisprudenza UE. Tale Comunicazione traduce così in termini concreti le regole vincolanti del GDPR e della pertinente giurisprudenza UE.

---

[23] Sull'esigenza di valorizzare l'uso dell'art. 114 TFUE anche G. CAGGIANO, *Competenze dell'Unione* cit., spec. p. 82. È invece dubitativa P. DE PASQUALE, *Le competenze dell'Unione europea* cit., spec. p. 2298. Sull'uso delle norme in materia di libera circolazione nel settore sanitario, v. anche Corte di giustizia, sentenza del 14 dicembre 2004, causa C-210/03, *Swedish Match*, punto 31 e B. DE WITTE, *Les competénces exclusives des Ètats members existent-elles?*, cit., p. 306.

[24] In tal senso, par. 2 (*Contributo delle app alla lotta al Covid-19*) della Comunicazione della Commissione europea del 17 aprile 2020, cit.; nonché i considerando 14 e 19 e le raccomandazioni 1 e 13 della raccomandazione della Commissione europea dell'8 aprile 2020 cit.

[25] Quanto al Comitato europeo per la protezione dei dati personali (EDPB), v. *Dichiarazione sul trattamento dei dati personali nel contesto della riapertura delle frontiere in seguito alla pandemia di Covid*-19, 16 giugno 2020, https://edpb.europa.eu/our-work-tools/our-documents/ovrigt/statement-processing-personal-data-context-reopening-borders_it.

[26] In merito, v. *Interoperability guidelines for approved contact tracing mobile applications in the EU* adottate dall'*eHealth network* del 13 maggio 2020, reperibili all'indirizzo https://ec.europa.eu/health/sites/health/files/ehealth/docs/contacttracing_mobileapps_guidelines_en.pdf.; e *Technical specifications for interoperability of contact tracing apps - eHealth Network Guidelines to the EU Member States and the European Commission on Interoperability specifications for cross-border transmission chains between approved apps*, 16 giugno 2020, https://ec.europa.eu/health/ehealth/key_documents_en#anchor0, nonché il comunicato stampa della Commissione europea, *Coronavirus: Gli Stati membri concordano una soluzione di interoperabilità per le applicazioni mobili di tracciamento e allerta*, 16 giugno 2020, https://ec.europa.eu/commission/presscorner/detail/it/ip_20_1043.

[27] Tali indicazioni sono state riprese e per tale via confermate nelle di poco successive linee guida 04/2020 del Comitato europeo per la protezione dei dati personali (EDPB) già cit., nonché nel *Joint Statement* del Consiglio d'Europa del 28 aprile 2020, parimenti volto a offrire agli Stati aderenti indicazioni sulla conformità di applicazioni di tracciamento con la Convenzione 108 e 108+ sulla protezione dei dati, https://rm.coe.int/covid19-joint-statement-28-april/16809e3fd.

2. La necessità di disporre di un'applicazione di tracciamento

Come già illustrato, le applicazioni di tracciamento, essendo fondate proprio sulla raccolta, la conservazione e l'uso dei dati personali degli individui, hanno una natura particolarmente intrusiva nella sfera privata dei singoli. A fronte di ciò, la Commissione europea, nella Comunicazione del 17 aprile 2020, ha raccomandato allora prima di tutto agli Stati membri di valutarne con serietà l'effettiva necessità di dotarsi di questi strumenti (principio di necessità di cui agli artt. 9 e 23 GDPR)[28].

La sussistenza di questo requisito deve essere effettuata da ciascun Paese membro, in funzione innanzitutto della capacità delle applicazioni di tracciamento d'interagire efficacemente con il sistema sanitario nazionale e, più in particolare, con l'abilità dello stesso di eseguire e processare *test* Covid-19 e scambiare i dati raccolti con le squadre di tracciamento umane. Un utente è avvisato del contatto con un certo soggetto attraverso la funzione di allerta propria di ogni applicazione di tracciamento solo quando quest'ultimo risulti infetto, condizione che dipende dall'esito di un apposito *test*[29]. La ridotta capacità di eseguire o processare questi ultimi in tempi brevi rende dunque inefficace la tempestiva allerta tramite le moderne tecnologie[30]. Il soggetto che sia stato avvisato del contatto col virus deve poi essere immediatamente inserito in un *iter* sanitario prevedibile che consenta di fornire in tempi rapidi a quest'ultimo chiare indicazioni di comportamento sia prima di effettuare il *test* Covid-19 (tempi e modalità dello stesso) sia in attesa dell'esito di quest'ultimo (quarantena o modalità di isolamento anche all'interno del domicilio se condiviso con altri), nonché a seguito della eventuale positività (monitoraggio progressivo dei sintomi; valutazione dello stato di salute anche di familiari; assistenza durante le cure soprattutto se al domicilio; tempi e modalità dei successivi *test* Covid-19 per valutare l'evoluzione della malattia). Ritardi nelle procedure sanitarie di gestione della malattia vanificano, infatti, parimenti gli effetti del tempestivo rilevamento dei potenziali soggetti infetti, i quali, in assenza di indicazioni, potrebbero anche adottare comportamenti inappropriati. Le informazioni raccolte con celerità dalle applicazioni in esame devono poi essere rese disponibili alle squadre di tracciamento. Inefficienze nel trasferimento dei dati tra i due pilastri del tracciamento – tecnologico e umano – portano, infatti, a duplicazioni del lavoro e ritardi difficilmente compatibili con la rapidità di diffusione della pandemia.

---

[28] Così, par. 1 (*Ambito degli orientamenti*) della Comunicazione della Commissione europea 17 aprile 2020, cit.

[29] Sulla correlazione tra *test* e efficacia delle applicazioni di tracciamento, par. 3.2 (*Garantire che la persona mantenga il controllo dei dati*) della Comunicazione della Commissione europea del 17 aprile 2020 cit., ove si legge che le autorità sanitarie possano avere accesso ai dati di una persona solo dopo la conferma che la persona interessata è realmente infettata al Covid-19 e a condizione che essa scelga di farlo.

[30] In tal senso, anche E. CIRONE, *L'app italiana di contact tracing* cit. e L. MC GREGOR, *Contact-tracing Apps and Human Rights*, 27 febbraio 2020, reperibile all'indirizzo https://www.ejiltalk.org/contact-tracing-apps-and-human-rights/?fbclid=IwAR1kIM0bYL8cHtw-nvLua48GoKlHiVV3r8glRD71CIH_R_ykETVLUMo9tYs.

Nonostante l'importanza di questi aspetti preliminari, l'art. 6 d.l. 28 non pare occuparsi, quantomeno espressamente, dei profili inerenti alla necessità di dotarsi di un'applicazione di tracciamento, concentrandosi invece su quelli di proporzionalità di cui si dirà nei prossimi paragrafi. Il comma 1 della disposizione in esame si limita, infatti, a stabilire che l'applicazione *Immuni* sarà impiegata per "*tutelare la salute attraverso le previste misure di prevenzione nell'ambito delle misure di sanità pubblica legate all'emergenza Covid-19*". Né invero un'analisi di dettaglio di questi aspetti è contenuta nei pareri resi dal Garante della *privacy* il 29 aprile 2020 sulla proposta normativa per la previsione di un'applicazione di tracciamento italiana o il 3 giugno 2020 quanto alla valutazione dell'impatto sulla protezione dei dati personali del trattamento degli stessi effettuato con *Immuni*[31]. Nel provvedimento del Garante del 1° giugno 2020 di autorizzazione al trattamento dei dati effettuato con *Immuni*, quest'ultimo ha inoltre solo confermato le osservazioni del Governo italiano quanto al "*particolare contesto emergenziale in cui il trattamento si inserisce e quindi con la necessità di adottare misure di contenimento del Covid-19 nel più breve tempo possibile*"[32].

L'assenza di valutazioni relative alla necessità di dotarsi di un'applicazione di tracciamento appare poi con maggior evidenza se paragonata al decreto francese 2020-650 del 29 maggio 2020 istitutivo dell'analoga applicazione *StopCovid* e ai pareri del Garante, ossia la *Commission informatique et liberté* (di seguito: CNIL)[33]. Le valutazioni del Governo francese si sono, infatti, fondate proprio sull'analisi di fattori inerenti alla capacità sanitaria basate sui pareri del Consiglio scientifico Covid-19 e dell'Accademia francese di medicina. La CNIL ha poi dedicato a questi profili l'*incipit* – peraltro intitolato proprio «*sur la nécessité…du dispositif*» – delle sue *déliberations* sia del 24 aprile 2020 sia del 25 maggio 2020. L'importanza attribuita a questi aspetti nel sistema francese emerge inoltre anche dal fatto che la CNIL, nella sua *déliberation* dell'8 maggio 2020, abbia precisato che la necessità del trattamento dei dati attraverso *StopCovid* debba essere periodicamente rivalutata in funzione dell'evoluzione dell'epidemia e delle conoscenza scientifiche[34]. Questa esigenza era stato peraltro già

[31] Rispettivamente, *Parere sulla proposta normativa per la previsione di una applicazione volta al tracciamento dei contagi da COVID-19 [9328050]* del 29 aprile 2020; *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* del 3 giugno 2020, www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9357972.

[32] V. in già citato *provvedimento di autorizzazione al trattamento dei dati personali effettuato attraverso il Sistema di allerta Covid-19 – App Immuni* del Garante del 1° giugno 2020.

[33] In aggiunta al *décret* 2020-650 del 29 maggio 2020 cit., CNIL, parr. 7-12 D*élibération 2020-046 du 24 avril 2020*, www.cnil.fr/sites/default/files/atoms/files/deliberation_du_24_avril_2020_portant_avis_sur_un_projet_dapplication_mobile_stopcovid.pdf; e i parr. 3-12 della *délibération 2020-056 du 25 mai 2020,* www.cnil.fr/sites/default/files/atoms/files/deliberation-2020-056-25-mai-2020-avis-projet-decret-application-stopcovid.pdf.

[34] La *Délibération 2020-051 du 8 mai 2020 portant avis sur un projet de décret relatif aux systèmes d'information mentionnés à l'article 6 du projet de loi prorogeant l'état d'urgence sanitaire,* in www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000041870579&categorieLien=cid.

manifestata dal *Conseil d'Etat* nell'*avis consultatif* reso al Governo sul progetto di legge di prolungamento dello stato di emergenza sanitaria in Francia del 4 maggio 2020[35].

3. Lo strumento giuridico sotteso all'adozione di applicazioni di tracciamento

Probabilmente al fine di provocare una seria riflessione sull'effettiva necessità di dotarsi di applicazioni di tracciamento, la Commissione europea, sempre nella sua Comunicazione del 17 aprile 2020, ha precisato che la decisione sull'adozione di strumenti di questo tipo e le loro condizioni di utilizzo dei dati sensibili ivi raccolti (art. 9, par. 2, lett. *i)* GDPR) sia assunta mediante un apposito strumento legislativo (art. 23 GDPR) con il coinvolgimento dei Garanti della *privacy* (artt. 35-36 GDPR). Al fine di rispettare gli artt. 9, 23, 35-36 GDPR, è allora prima di tutto necessario adottare una specifica normativa di base, essendo esclusa la possibilità di adattare al caso una previgente legislazione di diritto interno. In effetti, quest'ultima, adottata per finalità diverse dalla tutela della salute in situazioni non emergenziali, mal si adatterebbe alle peculiarità inerenti all'uso di strumenti particolarmente invadenti della sfera privata dei singoli in un contesto invece emergenziale. Anche tenuto conto della particolare sensibilità dei dati in discussione, ossia quelli relativi alla salute, solo l'uso di un'apposita normativa permetterebbe di regolamentare, e all'opinione pubblica di conoscere, il funzionamento e i limiti di funzionamento di tali strumenti – quanto, ad esempio, al tipo di dati personali raccolti, ai modi e ai tempi di raccolta e alla conservazione degli stessi, alle finalità del trattamento, all'identità del responsabile del trattamento cui rivolgersi per rettificare o cancellare i dati raccolti – in tal modo contribuendo a quella trasparenza così essenziale per il GDPR (artt. 5 e 12 ss.).

Nel rispetto delle indicazioni della Commissione europea, l'Italia ha adottato una specifica legislazione per disciplinare il funzionamento di *Immuni*, ossia il predetto art. 6 d.l. 28 del 30 aprile 2020 poi convertito nella legge n. 70 del 25 giugno 2020. Inoltre, come richiesto dall'art. 23 GDPR, il nostro Paese ha correttamente scelto di impiegare uno strumento di diritto interno di rango primario con il coinvolgimento del Parlamento. La Francia ha fatto una scelta analoga. Il già menzionato *décret* 2020-650 deputato a illustrare il funzionamento dell'applicazione di tracciamento *StopCovid* è in effetti stato sottoposto all'approvazione – ottenuta poi a giugno 2020 – del Parlamento francese ai sensi dell'art. 50-1 della Costituzione.

Pur se il d.l. 28 è adeguato agli standard UE dal punto di vista formale, esso non sembra tuttavia possedere un livello di dettaglio sostanziale pienamente conforme ai principi generali di cui agli artt. 5 e 12 GDPR e, più in generale, all'esigenza di consentire la totale comprensione del funzionamento di uno strumento tecnologico

[35] Spec. par. 7 del parewww.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9328050re del Consiglio di Stato francese del 29 aprile 2020, www.conseil-etat.fr/ressources/avis-aux-pouvoirs-publics/derniers-avis-publies/avis-sur-un-projet-de-loi-prorogeant-l-etat-d-urgence-sanitaire-et-completant-ses-dispositions.

particolarmente invasivo della sfera privata degli individui. Il d.l. 28 si occupa, infatti, di disciplinare il funzionamento di *Immuni* (e i suoi limiti) esclusivamente in un capo (il II) contenente un solo articolo (il n. 6), essendo la gran parte del decreto legge in esame (capo I) dedicata a un argomento diverso, ossia l'adozione di "misure urgenti in materia di intercettazioni di conversazioni dell'ordinamento penitenziario". Al fine di favorire la massima trasparenza di cui agli artt. 5 e 12 GDPR, sarebbe allora stato opportuno isolare la regolamentazione di *Immuni* in un atto distinto che ne dettagliasse peraltro la disciplina in una pluralità di disposizioni e che evitasse di lasciare la definizione di profili essenziali – il tipo di dati raccolti (par. 2, lett. *b*), il periodo di trattamento degli stessi (par. 2, lett. *e*) o la cessazione della durata del trattamento (par. 6) – a successivi (quanto indefiniti) interventi ministeriali. Sebbene l'uso dei decreti per completare la disciplina legislativa sia possibile e comprensibile, in Italia, come si avrà modo di vedere lungo tutto il corso del presente contributo, la piena comprensione del funzionamento di *Immuni* anche quanto ai profili sopra menzionati discende solo dalla lettura dell'art. 6 d.l. 28 alla luce dei, invece dettagliati, pareri del Garante del 29 aprile, 1° giugno e 3 giugno 2020. Più correttamente, il *décret* francese 2020-650 illustra invece il funzionamento di *StopCovid* in un unico e autonomo testo. Nonostante anche in questo caso sarebbe stato auspicabile un maggior dettaglio (il decreto francese si compone solo di sei disposizioni), il testo offre un quadro d'insieme più completo di quello italiano e le valutazioni della CNIL si aggiungono così a quelle legislative solo per precisarne il contenuto.

Quanto al coinvolgimento dei Garanti nella procedura di adozione delle applicazioni di tracciamento, è da rilevare il ruolo particolarmente attivo e l'elevata qualità dei pareri resi dal Garante italiano nel corso dell'intera procedura, così come richiesto dagli artt. 35 e 36 GDPR. Come dimostrato dai tre predetti pareri del 29 aprile, 1° giugno e 3 giugno 2020, quest'ultimo ha ripetutamente valutato l'applicazione *Immuni*, ossia già nella fase iniziale di riflessione sull'adozione dello strumento in esame, fornendo un primo parere sulla proposta normativa d'istituire un'applicazione di tracciamento italiana (29 aprile), analizzando poi lo strumento tecnologico in esame e suggerendo anche taluni opportuni aggiustamenti (1° giugno), nonché in ultimo valutando, come imposto dall'art. 35 GDPR nel caso di tracciamenti su larga scala, l'impatto dell'applicazione *Immuni* sulla protezione dei dati (3 giugno). Questi pareri sono poi estremamente dettagliati. Fatta eccezione per quello del 29 aprile 2020 che, essendo una prima valutazione della proposta di decreto legge, consta solo di quattro pagine, i successivi pareri del 1° giugno e del 3 giugno contano invece rispettivamente ben diciassette e undici pagine. Come già anticipato, a fronte della rilevata genericità dell'art. 6 d.l. 28, è stata proprio la lettura dei pareri del Garante a permettere di comprendere appieno il funzionamento (e soprattutto i limiti di funzionamento) della applicazione di tracciamento italiana. Considerata peraltro la particolare importanza attribuita dal GDPR ai Garanti, la quale è stata poi ulteriormente rafforzata nelle già

citate pronunce della Corte di giustizia *Schrems I* e *Schrems II*[36], non sorprende allora che un analogo elevato livello di coinvolgimento degli stessi nelle procedure di adozione di applicazioni Covid-19, nonché di qualità delle linee guida rese sia rinvenibile nella maggior parte degli Stati membri come, ad esempio, in Austria[37], Francia[38], Belgio[39] e Finlandia[40].

Quantomeno dall'analisi dei documenti a disposizione, non sembra invece che i Garanti nazionali siano stati sempre coinvolti nell'elaborazione e nell'adozione di applicazioni diverse da quelle di tracciamento soprattutto quando adottate a livello regionale (così, ad es., per l'applicazione di controllo dei sintomi *AlertLomb* della Regione Lombardia ad aprile 2020), il che lascia dubbi e perplessità sul corretto funzionamento di questi tipi di strumenti, nonché rischia di esporre gli Stati membri a (invece evitabili) procedure d'infrazione per l'errato comportamento delle proprie componenti amministrative[41].

4. Le finalità d'uso delle applicazioni tracciamento e dei dati personali ivi raccolti

Le legislazioni nazionali che istituiscono le applicazioni di tracciamento devono rispettare non solo il principio di necessità ma anche quello di proporzionalità (artt. 9 e 23 GDPR), il che presuppone innanzitutto l'impiego dei dati raccolti tramite gli strumenti in esame solo per conseguire obiettivi correlati al contrasto dell'emergenza

[36] Sul rafforzamento del ruolo dei Garanti in *Schrems I* cit., mi permetto di rinviare a S. CRESPI, *Il trasferimento dei dati personali UE in Stati terzi*, cit., p. 687 ss. Quanto a tali aspetti in *Schrems II* cit., v. tra i primissimi commenti alla sentenza del 16 luglio 2020 C. KUNER, *The Schrems II judgment of the Court of Justice and the future of data transfer regulation*, in *European Law Blog*, 17 luglio 2020; T. CHRISTAKIS, *After Schrems II : Uncertainties on the Legal Basis for Data Transfers and Constitutional Implications for Europe*, *Ibidem*, 21 luglio 2020.

[37] Quanto al ruolo del Garante in Austria, L. LINKOMIES, *Privacy is the hot issue*, cit., p. 10.

[38] Sul ruolo del CNIL in Francia, v. i già cit. pareri del 24 aprile 2020 e del 25 maggio 2020.

[39] In Belgio, il Garante ha reso l'a*vis* 36/2020 del 29 aprile 2020 reperibile sul sito dello stesso che ha sollecitato il Governo ad introdurre svariati cambiamenti alle due proposte di regi decreti di aprile 2020 quanto all'adozione di un'applicazione di tracciamento anche in tale Stato membro. Al momento in cui si scrive, non pare che il Belgio abbia ancora reso operativo uno strumento di questo tipo, il quale pare però previsto per l'autunno 2020.

[40] Quanto alla Finlandia, v. *Bulletin n. 2* dell'agenzia europea FRA di aprile 2020, cit., spec. p. 52.

[41] In merito, v. il generale (e generico) riferimento del Garante della *privacy* italiano di cui al *Parere sulla proposta normativa* cit. del 29 aprile 2020 (p. 4) secondo cui "l'Autorità auspica che tale misura [l'adozione di un'applicazione nazionale adeguata al GDPR con l'aiuto del Garante stesso] sia idonea anche a superare il proliferare di iniziative analoghe in ambito pubblico, difficilmente compatibili con il quadro giuridico vigente". Sull'applicazione della Regione Lombardia e la vaghezza delle regole GDPR anche BOEHM, DIMITROVA, PICHIERRI, HALLINAN, *Tracking and Tracing Apps and data protection in the context of the Covid-19 pandemic: Data protection requirements and recommendations for the deployment of Covid-19 tracking and tracing apps*, FIZ Karlsruhe, Aprile 2020, www.fiz-karlsruhe.de/sites/default/files/FIZ/Dokumente/FIZnews/tracking_app_EN_20200428.pdf. L'adozione di applicazioni di tracciamento regionali solleva peraltro dubbi anche di costituzionalità relativi alla ripartizione di competenze tra Stato e regioni. In tal senso, G. TROPEA, *Il contact tracing digitale e l'epidemia: sindrome cinese?* disponibile in www.lacostituzione.info del 9 aprile 2020, facendo riferimento a Consiglio di Stato, sez. I, sentenza del 7 aprile 2020, n. 735, nonché G. DELLA MORTE, *Quanto Immuni? Luci, ombre e penombre dell'app selezionata dal Governo italiano*, cit., spec. p. 319.

sanitaria in corso (artt. 5, lett. *b)*, 6, par. 4, e art. 9, par. 2, GDPR). È dunque esclusa la possibilità di usare le dette applicazioni per raccogliere, conservare e utilizzare i dati degli utenti per scopi diversi o ulteriori come, ad esempio, il controllo dell'immigrazione, la sicurezza nazionale o per finalità commerciali, permettendone l'accesso o il trasferimento a soggetti terzi (c.d. trasferimenti secondari).

Conformemente alle indicazioni del GDPR ribadite dalla Commissione nella sua Comunicazione, l'art. 6, comma 1, d.l. 28 limita l'uso di *Immuni* alle finalità di interesse pubblico di "allertare le persone che siano entrate in contatto stretto con soggetti risultati positivi e tutelarne la salute attraverso le previste misure di prevenzione nell'ambito delle misure di sanità pubblica legate all'emergenza Covid-19". Tuttavia, considerata l'importanza di quest'aspetto, sarebbe stato opportuno non limitarne l'individuazione al solo *incipit* del comma 1 dell'art. 6, ma dedicarvi un'apposita norma, così come peraltro fatto in Francia all'art. 1 *décret* 2020-650. Ciò avrebbe permesso anche d'individuare con maggior precisione gli esatti confini delle finalità del trattamento sottese all'applicazione *Immuni.* Non è, ad esempio, chiaro in che modo si sostanzi la menzionata "tutela della salute attraverso le previste misure di prevenzione" di cui al comma 1 dell'art. 6 d.l. 28. Ai soggetti allertati sono fornite solo linee direttrici in materia di prevenzione o saranno invece seguiti dai servizi sanitari? Le indicazioni fornite sono facoltative o obbligatorie? In che modo e tempi essi saranno sottoposti ad apposito *test* per valutare la loro positività al Covid-19, il quale è un presupposto essenziale per avviare la funzione di allerta delle applicazioni di tracciamento? La mancanza di dettagli quanto a questi aspetti è ancora più evidente paragonando il comma 1 dell'art. 6 d.l. 28 al par. 2 dell'art. 1 del decreto francese 2020-650. Nell'individuare le funzioni di *StopCovid*, la disposizione francese precisa, infatti, che l'applicazione di tracciamento è volta a *a)* informare gli utenti che esiste il rischio di essere stati infettati in ragione del loro contatto prossimo con un altro utilizzatore diagnosticato positivo al Covid-19; *b)* sensibilizzare gli utenti, e in particolare quelli esposti al contagio e allertati, sui sintomi del virus e la condotta da tenere per contenere la propagazione del contagio; *c)* raccomandare ai contatti a rischio di orientarsi verso un certo operatore sanitario, il quale funge così da guida consigliando sui comportamenti da adottare in funzione dei sintomi.

L'impossibilità d'utilizzare i dati raccolti con applicazioni di tracciamento per scopi ulteriori o diversi da quelli indicati nella legislazione istitutiva degli strumenti in esame è integrata nel nostro Paese dall'uso, all'*incipit* del comma 1 dell'art. 6 d.l. 28, dei termini "al solo fine di". La lista di finalità di trattamento ivi individuate – "allertare le persone che siano entrate in contatto stretto con soggetti risultati positivi e tutelarne la salute attraverso le previste misure di prevenzione nell'ambito delle misure di sanità pubblica legate all'emergenza Covid-19" – è allora tassativa ed esaustiva. Ciò trova conferma anche al comma 3 della medesima disposizione ove si ribadisce che "i dati raccolti attraverso l'applicazione di cui al comma 1 non possono essere trattati per finalità diverse da quella di cui al comma 1". Il fatto poi che, come suggerito dalla

Commissione europea nella Comunicazione del 17 aprile 2020[42] e in conformità all'art. 28 GDPR, l'Italia – come peraltro la Francia al par. 1 dell'art. 1 *décret* 2020-650 – abbia individuato, al comma 1 dell'art. 6, nel Ministero della salute il responsabile del trattamento, conferma una volta di più la volontà di limitare anche per il futuro il predetto trattamento dei dati a scopi solo inerenti alla tutela della salute pubblica.

Quanto ai trattamenti secondari che, per la Commissione europea, dovrebbero essere sempre evitati, il d.l. 28 (e anche il decreto francese) non contiene un'esplicita esclusione. Anzi, il fatto che il comma 3 dell'art. 6 del d.l. 28 preveda che i dati raccolti con *Immuni* potranno essere impiegati per fini statistici e di ricerca una volta conclusa l'emergenza sanitaria, sembra proprio ammettere un loro uso successivo ad opera di soggetti diversi dal Ministero della salute. Nonostante ciò, il Garante italiano, in modo non perfettamente comprensibile, ha invece dedotto dalla lettura congiunta dei commi 1 e 3 dell'art. 6 d.l. 28 l'impossibilità di ogni trattamento secondario[43]. Inoltre, pur se, come rilevato dal nostro Garante, la conformità al GDPR di prescrizioni come quella del comma 3 è assicurata dall'uso dei dati in forma anonima e aggregata (art. 89 GDPR)[44], al fine di eliminare ogni dubbio su ulteriori trattamenti, sarebbe stato opportuno precisare i soggetti che avranno accesso a tali dati (solo le autorità sanitarie elencate al comma 1 dell'art. 6 o anche altri enti terzi?) o prevedere uno specifico consenso da parte degli utenti.

La volontà di evitare ogni uso improprio delle applicazioni di tracciamento è rinvenibile anche nella richiesta della Commissione europea d'inserire nelle legislazioni istitutive degli strumenti in esame l'esplicita esclusione dell'uso ad opera di autorità pubbliche nazionali dei dati personali raccolti e conservati per realizzare una sorveglianza di massa[45]. Un riferimento del genere non è tuttavia contenuto né nella legislazione italiana né in quella francese, il che ha indotto quantomeno il Garante di quest'ultimo Stato membro a precisare nel suo parere del 25 maggio 2020 che il trattamento dei dati raccolti con *StopCovid* non dovrebbe mai consentire il monitoraggio delle interazioni sociali delle persone.

L'assenza di ogni menzione del divieto di sorveglianza di massa nel d.l. 28 e/o nei pareri del Garante italiano preoccupa, considerato che l'Unione europea è già stata confrontata a esperienze di questo tipo nei casi *Schrems I* (sorveglianza di massa sui dati UE trasferiti negli USA)[46] e in alcuni Paesi membri principalmente dell'Est Europa. A titolo esemplificativo, l'Ungheria, pur non disponendo di applicazioni per contrastare l'emergenza sanitaria in corso, a fine marzo 2020 ha modificato alcune leggi che autorizzano ora le autorità di polizia, immigrazione e sanitarie a chiedere (e ottenere) dagli operatori nazionali i dati di localizzazione dei residenti senza il previo consenso

[42] Par. 3.1 (*Le autorità sanitarie nazionali (o i soggetti che svolgono compiti nel pubblico interesse nel campo della salute) come titolari del trattamento)* della Comunicazione della Commissione europea del 17 aprile 2020 cit.
[43] Così, art. 6, co. 1, d.l. 28 cit. e il parere del Garante italiano del 29 aprile 2020, cit.
[44] In tal senso, parere del Garante italiano del 29 aprile 2020, cit., spec. p. 4.
[45] In tal senso, par. 1 (*Contesto*) della Comunicazione della Commissione europea del 17 aprile 2020 cit.
[46] Corte di giustizia, *Schrems* I, cit. e la dottrina ivi cit.

dell'interessato e né autorizzazioni della magistratura[47]. In Polonia vige inoltre l'obbligo per coloro che si trovino in quarantena d'installare sul proprio dispositivo mobile un'applicazione che informa le autorità di polizia della localizzazione degli stessi, così da poter accertare e sanzionare il rispetto delle misure di confinamento[48]. L'adozione di legislazioni e applicazioni di tale genere, andando chiaramente oltre ciò che è necessario per contrastare la pandemia, espone tali Stati membri al concreto rischio di procedure di infrazione per violazione non solo delle disposizioni UE in materia di tutela dei dati, ma anche dell'art. 2 TUE[49]. Il fatto peraltro che esse mettano in discussione i valori fondanti l'UE espone questi ultimi anche alla procedura di cui all'art. 7 TUE, in ogni caso già avviata rispettivamente dal Parlamento europeo e dalla Commissione europea nei confronti di Ungheria e Polonia per le ripetute e pregresse violazioni[50]. La gravità dei comportamenti in atto in tali Paesi membri nel periodo Covid-19 potrebbe allora spingere il Consiglio e il Consiglio europeo – fino ad ora inerti per ragioni politiche – a una presa di posizione *ex* art. 7 TUE.

La previsione in Italia e Francia dell'espressa esclusione di una sorveglianza di massa avrebbe poi mitigato la scelta nazionale di conservare i dati raccolti con la predetta applicazione in un *server* nazionale centrale (sistema centralizzato di cui si dirà oltre al par. 6), la quale, rispetto alla conservazione decentrata suggerita dalla Commissione europea in quanto più conforme al principio di minimizzazione di cui agli artt. 5 e 25 GDPR, per natura permette un più facile accesso ai dati ad opera di autorità pubbliche e dunque eleva proprio il rischio di una sorveglianza di massa.

5. L'uso solo temporaneo delle applicazioni di tracciamento e dei dati personali ivi raccolti

Al fine di rispettare il principio di proporzionalità (artt. 9 e 23 GDPR) e favorire lo stretto collegamento richiesto dalla Commissione europea tra applicazioni di

[47] Così, il più volte già citato *Bulletin n. 2* dell'agenzia FRA di aprile 2020, spec. pp. 52-53. Il testo della legge è rinvenibile in *questionegiustizia.it*, seppur in una traduzione italiana non ufficiale.

[48] I. A. HAMILTON, *Poland made an app that forces coronavirus patients to take regular selfies to prove they're indoors or face a police visit*, https://www.businessinsider.com/poland-app-coronavirus-patients-mandaotory-selfie-2020-3?IR=C.

[49] Sulle numerose infrazioni dell'Ungheria, Corte di giustizia, sentenza del 6 novembre 2012, *Commissione c. Ungheria*, causa C-286/12, ECLI:EU:C:2012:687; nonché il ricorso per infrazione del 20 dicembre 2019, causa C-821/19, ancora pendente davanti alla Corte In merito, anche i comunicati stampa della Commissione europea relativi ai casi IP/17/5003, IP/17/5004 e IP/1975994. Sull'argomento *ex multis* in dottrina, E. CANNIZZARO, *Il ruolo della Corte di giustizia nella tutela dei valori dell'Unione europea*, in Liber amicorum *Antonio Tizzano. De la Cour CECA à la Cour de l'Union: le long parcours de la justice européenne*, Torino, 2018, p. 158 ss; P. MORI, *L'uso della procedura d'infrazione a fronte di violazioni dei diritti fondamentali*, in *Il diritto dell'Unione europea*, 2018, p. 363 ss.

[50] Risoluzione del Parlamento europeo del 23 dicembre 2019, in GUUE C 433, spec. p. 66. In generale sugli artt. 2 e 7 TUE, E. LEVITS, *L'Union européenne en tant que communauté de valeurs partagées. Les conséquences juridiques des articles 2 et 7 TUE pour les Etats membres*, in Liber amicorum *Antonio Tizzano. De la Cour CECA à la Cour de l'Union: le long parcours de la justice européenne*, Torino, 2018, p. 509 ss.

tracciamento e lotta al Covid-19, l'uso degli strumenti in esame e dei dati personali ivi raccolti deve essere temporalmente circoscritto alla sola emergenza sanitaria in corso, dovendo le applicazioni di tracciamento essere disattivate e i dati ivi raccolti cancellati "al più tardi quando la pandemia sia dichiarata sotto controllo" (*sunset clause* di cui all'art. 5 GDPR)[51]. Se l'uso di questi strumenti è motivato (o dovrebbe esserlo) dalla sola volontà di contrastare la pandemia, la cessazione della stessa dovrebbe far venire meno l'utilità delle applicazioni. Il rispetto di questa condizione permette anche di ridurre il rischio di un uso improprio da parte delle autorità pubbliche dei dati personali raccolti dalle applicazioni in esame e/o dei casi di sorveglianza di massa. Tali dati non sarebbero in effetti più accessibili alla fine dell'emergenza, il che eliminerebbe o ridurrebbe il rischio di un loro uso per finalità ulteriori a quelle sanitarie.

La trasposizione di questa condizione nel nostro Paese non pare tuttavia essere stata pienamente soddisfacente. Il termine di cessazione del trattamento dei dati raccolti con applicazioni di tracciamento – da individuare, per la Commissione, in base a un parametro epidemiologicamente oggettivo, ossia "quando la pandemia sia dichiarata sotto controllo" – è stato individuato all'art. 6, comma 6, d.l. 28 (e anche in Francia all'art. 3 *décret* 2020-650) alla conclusione dello stato di emergenza nazionale, il quale è stato decretato in Italia con delibera dal Consiglio dei ministri poi approvata in Parlamento[52] . Essendo la dichiarazione di stato di emergenza (e anche la sua cessazione o la sua proroga) una scelta essenzialmente governativa, l'interruzione del trattamento dei dati attraverso *Immuni* varia allora in funzione di un fattore puramente discrezionale difficilmente prevedibile e non invece in virtù di un parametro oggettivamente connesso alla pandemia, da valutarsi in base a soglie e valori clinici prestabiliti come voluto dalla Commissione europea. La scelta italiana potrebbe allora essere considerata proporzionata solo qualora la legislazione sullo stato di emergenza stabilisca la cessazione di questa condizione – e dunque anche del trattamento dei dati tramite le predette applicazioni – in funzione di parametri non discrezionali inequivocabilmente connessi all'emergenza sanitaria, il che tuttavia non pare essere il caso, quantomeno a livello legislativo, in Italia (e anche in Francia) [53]. Né invero tale discrezionalità pare limitata dal fatto che l'art. 6, comma 6, d.l. 28 precisi che il trattamento dei dati attraverso l'applicazione *Immuni* si concluderà "in ogni caso al più tardi il 31 dicembre 2020", ben potendo questa data essere prorogata alla scadenza. Il fatto poi che il funzionamento di *Immuni* sia connesso allo stato di emergenza potrebbe indurre il Governo a prorogare quest'ultimo oltre ciò che è normalmente consentito proprio per

[51] Così, par. 1, (*Contesto*), della Comunicazione della Commissione europea del 17 aprile 2020 cit.

[52] Quanto all'Italia, la *Dichiarazione dello stato di emergenza in conseguenza del rischio sanitario connesso all'insorgenza di patologie derivanti da agenti virali trasmissibili*, 20A00737, è pubblicata in GU 26 del 1° febbraio 2020. Per la Francia, *loi n° 2020-290 d'urgence pour faire face à l'épidémie de covid-19* del 23 marzo 2020, reperibile in www.legifrance.gouv.fr/affichTexte.do;jsessionid=84A11ADD878E9B78D802D901D1B13966.tplgfr34s_2?cidTexte=LEGITEXT000041746988&dateTexte=20200711.

[53] Non si può in effetti escludere che in concreto lo stato di emergenza sia definito in funzione di parametri sanitari ad es. quelli della *Roadmap*, https://ec.europa.eu/info/sites/info/files/communication_-_a_european_roadmap_to_lifting_coronavirus_containment_measures_0.pdf.

permettere il funzionamento del predetto strumento di tracciamento, il quale per natura esplica la propria funzionalità e massimizza la sua utilità nella fase di contenimento e di controllo della pandemia e dunque quando la situazione emergenziale in senso stretto è ormai alle spalle.

Anche per tutelare le parti deboli della società che, per scarsa dimestichezza con la tecnologia, abbiano difficoltà a installare, usare e disinstallare le applicazioni, la Commissione europea richiede poi che quest'ultima operazione non dipenda dall'iniziativa del singolo utente, dovendo essere realizzata dall'esterno nei confronti di tutti gli utenti "al più tardi quando la pandemia sia dichiarata sotto controllo" [54]. Il fatto che il comma 6 dell'art. 6 del d.l. 28 preveda che "l'utilizzo dell'applicazione e della piattaforma, nonché ogni trattamento di dati…sono interrotti alla data di cessazione dello stato di emergenza…o al più tardi il 31 dicembre 2020", senza richiedere cioè alcuna attività degli utenti, sembra attestare la conformità dello stesso alle indicazioni UE, prevedendo, entro il predetto *expire time*, la disinstallazione simultanea ed esterna dell'applicazione *Immuni*.

6. Il mantenimento del controllo sulle applicazioni di tracciamento e sui dati ivi raccolti: volontarietà, uso di *Bluetooth* e conservazione decentrata

Nella Comunicazione del 17 aprile 2020, la Commissione europea ha suggerito una serie di salvaguardie finalizzate a favorire il mantenimento del controllo delle applicazioni di tracciamento e dei dati ivi raccolti ad opera dei singoli utenti[55]. A tal fine, l'installazione delle applicazioni sul dispositivo mobile degli utenti deve innanzitutto avvenire su base volontaria e senza conseguenze negative per la persona che decide di non scaricare o usare l'applicazione, non potendo neppure il datore di lavoro imporne al dipendente l'installazione[56]. Tale indicazione è stata correttamente trasposta nel d.l. 28, essendo la volontarietà di *Immuni* prevista espressamente al comma 1 dell'art. 6. Al fine di evidenziarne la piena discrezionalità, il comma 4 della medesima norma precisa poi che il mancato uso dell'applicazione "non comporta alcuna conseguenza pregiudizievole". L'analisi comparata dei sistemi nazionali mostra come questa condizione sia stata rispettata da tutti gli Stati membri che hanno adottato o hanno scelto di dotarsi in futuro di applicazioni di tracciamento[57], essendo viceversa prevista l'obbligatorietà della stessa solo in Cina, Taiwan e Qatar.

A differenza tuttavia del decreto francese che dedica particolare attenzione alla volontarietà di *StopCovid* in ogni fase del funzionamento della stessa (artt. da 1 a 4 del decreto francese 2020-650), il legislatore italiano, quantomeno formalmente, si limita a

[54] In tal senso, par. 3.2 (*Garantire che la persona mantenga il controllo*) della Comunicazione della Commissione europea del 17 aprile 2020, cit.
[55] Così, par. 3.2 (*Garantire che la persona mantenga il controllo*), *ibidem*.
[56] V. par. 3.3 (*Base giuridica per il trattamento*), *ibidem*.
[57] In merito, *Bulletin n. 2* dell'agenzia europea FRA di aprile 2020, cit., p. 48 ss.

prevedere tale caratteristica solo al momento dell'installazione di *Immuni*. Questa lacuna è stata rilevata anche dal nostro Garante, il quale ne ha chiesto l'adeguamento nel già citato parare del 1° giugno 2020. Un'applicazione fondata sulla volontarietà degli utenti implica, infatti, che la volontà si manifesti in tutte le parti di funzionamento: *download*, installazione, configurazione, attivazione della tecnologia *Bluetooth*, caricamento delle TEK sul *backend* in caso di risultato positivo del tampone, raccolta delle diverse categorie di *analytics* nelle fasi in cui si articola il trattamento, consultazione del medico dopo aver ricevuto un messaggio di allerta sul rischio di essere entrato in contatto con positivi e disinstallazione dell'applicazione[58].

Inoltre, a differenza di altri Stati (Bulgaria, Cipro, Slovenia e Lituania)[59], il nostro Paese ha parimenti correttamente recepito l'ulteriore indicazione della Commissione europea d'impiegare la modalità *Bluetooth* a bassa energia (BLE) in luogo di quella GPS[60], in quanto più conforme ai principi di minimizzazione, *privacy by design* e *privacy by default* di cui all'art. 25 GDPR. A differenza del *Bluetooth* che utilizza i dati generati dallo scambio di segnali tra dispositivi mobili e permette così di tracciare i contatti tra individui sulla base della sola prossimità dei segnali (c.d. *contact tracing*), il GPS funziona in base all'esatta localizzazione dell'utente ed è allora utile nel caso in cui il tracciamento sia volto a seguire i movimenti di un certo individuo o a fare rispettare prescrizioni come la quarantena (c.d. *location tracing*). Applicazioni che impieghino questa seconda tecnologia vanno allora oltre a quanto necessario per individuare i soggetti entrati in contatto con il virus – essendo a tal fine sufficiente la prossimità dei contatti – e dunque con i predetti principi del GDPR, fornendo in un certo senso dati sovrabbondanti.

Sempre al fine di garantire il controllo degli utenti sui propri dati personali, la Commissione europea suggerisce poi che i dati di prossimità generati dallo scambio di segnali *Bluetooth* tra dispositivi mobili debbano essere conservati – in forma criptata associando identificativi pseudonimi o anonimi generati arbitrariamente a partire dal numero di telefono immesso al momento dell'attivazione dell'applicazione – sul dispositivo mobile dell'utilizzatore (conservazione decentrata o distribuita) e non in *server* nazionali (conservazione centralizzata)[61]. Pur se entrambe le soluzioni mostrano pregi e difetti[62] e la distinzione tra i due modelli non sia sempre così netta[63], la soluzione decentrata avrebbe più di altre il merito di garantire all'utilizzatore il controllo

[58] V. Parere del Garante italiano del 1° giugno 2020, cit., spec. punto 1.1 a p. 7.
[59] In tal senso, *Bulletin n. 2* dell'agenzia europea FRA di aprile 2020, cit., p. 48 ss.
[60] Così, par. 3.2 (*Garantire che la persona mantenga il controllo*) della Comunicazione della Commissione europea del 17 aprile 2020, cit.
[61] Par. 3.4 (*Minimizzazione dei dati*), *ibidem*.
[62] Così, F. BAIARDI, *Le proprietà di un sistema per il tracing: centralizzato, decentralizzato, open source*, https://www.riskmanagement360.it/analisti-ed-esperti/le-proprieta-di-un-sistema-per-il-tracing-centralizzato-decentralizzato-open-source. Ciò aveva così indotto sia l'EDPB (linee guida 04/2020 del 21 aprile 2020 cit., punto 42) sia il Garante italiano (valutazione d'impatto del 3 maggio 2020 cit.) a ritenere che, in linea di principio, le applicazioni di tracciamento potessero seguire un approccio sia centralizzato sia decentrato.
[63] In tal senso, la valutazione d'impatto del Garante italiano del 3 maggio 2020, cit., pp. 2-3.

sui dati – i quali sono per l'appunto conservati sul proprio dispositivo mobile e non in *server* esterni – nonché di esporre meno il sistema ad attacchi cibernetici a fronte, ancora una volta, della conservazione solo locale dei dati. Il sistema decentrato permette inoltre di ridurre il rischio di sorveglianza di massa ad opere delle autorità pubbliche, la quale ben potrebbe essere agevolata dalla conservazione di tutti i dati degli utenti in un unico *server* nazionale[64].

Nonostante le chiare indicazioni UE sull'uso di sistemi decentrati e le perplessità sul modello centralizzato rilevate anche dal Parlamento europeo e dalla gran parte dell'accademia e dalle ONG[65], un po' sorprendentemente l'Italia ha scelto di optare – insieme a Austria, Belgio, Bulgaria, Danimarca, Francia, Lituania, Slovacchia e Repubblica ceca – per il sistema centralizzato. In realtà, tale ricostruzione è stata contestata dal nostro Garante. Secondo quest'ultimo, il fatto che l'art. 6, comma 2, lett. *e*) d.l 28 preveda che "i dati relativi ai contatti stretti siano conservati *anche nei dispositivi mobili degli utenti*" sottintenderebbe la scelta dell'Italia per un sistema c.d. semi-decentrato[66]. Sul presupposto che anche nei modelli distribuiti sia presente una componente centrale, il sistema italiano – nella misura in cui prevede che solo l'accertamento dello stato di salute sia effettuato centralmente, essendo invece svolta localmente la verifica degli avvenuti contatti con i positivi a mezzo del confronto tra pseudonimi sugli *smartphone* – si differenzierebbe allora dai modelli totalmente centralizzati, in cui entrambi gli adempimenti vengono effettuati per l'appunto centralmente. Pur nell'incertezza iniziale sul modello da impiegare a cui si è fatto cenno, le indicazioni della Commissione europea quanto all'uso di sistemi distribuiti avrebbero tuttavia dovuto orientare, anche solo in un secondo tempo, il nostro Paese verso questo sistema, così come peraltro avvenuto in Germania anche per effetto delle forti critiche interne[67]. Ciò è a maggior ragione vero considerato che, come rilevato dal Garante italiano e da una parte della dottrina[68], il riferimento di cui al par. 2, lett. *e)* del d.l. 28 alla circostanza per cui i dati "relativi ai contatti stretti siano conservati, anche nei dispositivi mobili degli utenti" lascia incertezze – e dunque si espone a criticità – quanto al regime di comunicazione tra dispositivi mobili e server.

---

[64] Pur concordando sulla maggior compatibilità del Bluetooth con il GDPR, G. DELLA MORTE, *Quanto Immuni? Luci, ombre e penombre dell'app selezionata dal Governo italiano*, cit. spec. p. 310 rileva come tale tecnica, in quanto meno precisa di quella GPS, possa determinare un numero superiori di rilevamenti falsi positivi o falsi negativi.

[65] Quanto al Parlamento europeo, risoluzione del 17 aprile 2020, *EU Coordinated action to combat the COVID-19 pandemic and its consequences*, (2020/2616(RSP)), spec. par. 52, nonché la dottrina citata nel *Bulletin n. 2* dell'agenzia europea FRA cit. alla nota 211.

[66] In tal senso, la valutazione d'impatto del Garante italiano del 3 giugno 2020 cit., spec. il paragrafo sulle scelte architetturali di modellazione dei dati, pp. 1-2. G. DELLA MORTE, *Quanto Immuni? Luci, ombre e penombre dell'app selezionata dal Governo italiano*, cit., spec. p. 323 rileva poi la criticità dell'inciso in esame anche quanto all'indeterminatezza del regime di comunicazione tra dispositivi e server.

[67] In merito, L. LINKOMIES, *Privacy is the hot issue*, cit., p. 10 ss.

[68] In tal senso, la già più volte citata valutazione di impatto del nostro Garante del 3 giugno 2020, punto "*Migliorie tecniche specifiche*" a p. 8, nonché in dottrina G. DELLA MORTE, *Quanto Immuni? Luci, ombre e penombre dell'app selezionata dal Governo italiano*, cit., spec. p. 323.

Qualunque sia il sistema – distribuito o centralizzato – prescelto da un certo Stato, la Commissione europea richiede poi che l'accesso delle autorità pubbliche ai dati raccolti tramite applicazioni di tracciamento avvenga a una duplice condizione, ossia dopo aver accertato l'effettiva positività dell'utilizzatore al Covid-19, e aver ottenuto da quest'ultimo un apposito consenso (6 GDPR)[69], il quale deve poi essere libero, specifico, esplicito e informato, nonché espresso mediante un'azione positiva inequivocabile[70]. È allora esclusa ogni forma di consenso tacito come il silenzio o l'inattività. Sebbene sia ragionevole pensare che un soggetto che abbia scelto di installare un'applicazione di tracciamento sul proprio dispositivo mobile sia anche propenso, una volta risultato infetto, a dare accesso ai dati personali raccolti con la predetta applicazione, il mero consenso apposto al momento dell'installazione della stessa non è correttamente considerato sufficiente a permettere un automatico accesso delle autorità pubbliche ai dati ivi raccolti.

Ora, seppur in maniera troppo sintetica, i commi 1 e 2 lett. *b*) dell'art. 6 d.l. 28 limitano correttamente la funzione di allerta di *Immuni* e il trattamento dei dati ivi raccolti ai soli soggetti entrati in contatto con individui accertati positivi al Covid-19. In particolare, il comma 1 della disposizione in esame prevede che *Immuni* abbia come funzione essenziale quella di "allertare le [sole] persone che siano *entrate in contatto stretto con soggetti risultati positivi*", e la lett. *b)* del comma 2 della stessa circoscrive l'uso dei "dati personali raccolti dall'applicazione…esclusivamente [a] quelli necessari ad avvisare gli utenti dell'applicazione di rientrare tra i contatti stretti di altri utenti *accertati positivi al COVID-19*". Il d.l. 28 non affronta la questione, invece essenziale, dei tempi e dei modi in cui sarà richiesto e prestato dall'utente il consenso all'accesso ai propri dati ad opera dalle autorità pubbliche nazionali (così anche nel decreto francese 2020-650). Né invero il Garante italiano, pur così attento lungo tutta la procedura di adozione di *Immuni*, pare aver rilevato tale vuoto legislativo.

7. Il tipo di dati personali raccolti con le applicazioni di tracciamento e la durata della loro conservazione

In virtù del principio di minimizzazione di cui agli artt. 5 e 25 GDPR, la Commissione europea ricorda che possono essere trattati solo i dati adeguati, pertinenti e limitati a quanto effettivamente necessario, i quali variano peraltro in funzione delle finalità dell'applicazione (informativa o di controllo dei sintomi e/o di tracciamento).

[69] Alcune prestigiose istituzioni di ricerca come l'*INRIA* in Francia (www.inria.fr/fr/contact-tracing-bruno-sportisse-pdg-dinria-donne-quelques-elements-pour-mieux-comprendre-les-enjeux) e la *Fraunhofer-Gesellschaft* in Germania (www.fraunhofer.de/content/dam/zv/en/press-media/2020/april/fraunhofer-paper-proximity-tracing-in-the-context-of-coronafraunhofers-approach-for-germany.pdf) hanno contestato il modello decentralizzato sostenendo che l'invio di informazioni relative a tutti gli utenti positivi costituisca un rischio in sé, in quanto tali informazioni potrebbero consentire a utenti maliziosi del sistema di re-identificarli.

[70] Così, par. 3.3 (*Base giuridica del trattamento*) della Comunicazione della Commissione europea del 17 aprile 2020, cit.

Qualora un certo Stato membro abbia poi deciso di dotarsi di questo ultimo tipo di applicazioni, i dati utili, anche sulla base di quanto già illustrato, devono prima di tutto essere solo quelli di prossimità tra utenti (*Bluetooth*) e non quelli di esatta ubicazione degli utilizzatori (*GPS*). Considerato inoltre che i dati trasmessi dall'applicazione devono includere esclusivamente identificatori univoci e pseudonimi da rinnovarsi secondo una frequenza compatibile con lo scopo di contenere la diffusione del virus e sufficiente a limitare il rischio di identificazione e di localizzazione fisica delle persone, l'applicazione non dovrebbe neppure raccogliere i dati anagrafici, gli identificativi di comunicazione, le voci di *directory* del dispositivo mobile, i messaggi o le registrazioni di chiamate[71]. Il principio di minimizzazione suggerisce inoltre l'irrilevanza della conservazione dell'ora del contatto e invece la rilevanza del giorno del contatto così da poter stabilire, anche in base allo stadio di evoluzione della malattia del diffusore, il periodo di quarantena[72].

Nonostante le indicazioni di dettaglio fornite dalla Commissione europea, l'art. 6, comma 2, let. *b*) d.l 28 si limita a stabilire che "i dati raccolti…siano esclusivamente quelli necessari ad avvisare gli utenti...di rientrare tra i contatti stretti di altri utenti accertati positivi al COVID-19". Inoltre, la lett. *c*) della medesima disposizione precisa, come richiesto dalla Commissione europea, che "è esclusa…la geo-localizzazione dei singoli utenti". L'esatta individuazione dei dati conservati e trattati è lasciata a un successivo (quanto imprecisato) intervento del Ministero della salute. È in effetti solo alla luce delle indicazioni di dettaglio illustrate dal Garante della *privacy* nel suo parere del 1° giugno 2020 che emerge la generale conformità del sistema di conservazioni dei dati italiano al principio di minimizzazione di cui gli artt. 5 e 25 GDPR[73] quanto ai dati utili sia per tracciare e allertare le persone che siano entrate in contatto con il virus (ad es., TEK, RPI, data di inizio dei sintomi per persone positive e dell'avvenuta ricezione della notifica di esposizione) sia per fini di sanità pubblica e di miglioramento del sistema (ad es., provincia di domicilio, data in cui è avvenuto l'ultimo contatto a rischio, grado di rischio di contagio, l'aver ricevuto un messaggio di allerta, lo stato di attivazione del *bluetooth*, il sistema operativo del dispositivo, il *clock* del dispositivo, gli *analytics token* e i *device token*).

Un medesimo livello di genericità è da rilevarsi quanto alla durata della conservazione dei dati personali raccolti tramite le applicazioni di tracciamento, la quale, sempre in virtù degli artt. 5 e 25 GDPR, non può essere più lunga di quanto necessario ed è da determinarsi in base alle funzionalità dell'applicazione (ad. es., informativa o di controllo dei sintomi e/o di tracciamento)[74]. Nonostante la Commissione europea, nella sua Comunicazione del 17 aprile 2020, avesse indicato per

[71] In tal senso, punto 3.2 delle linee guida 04/2020 del 21 aprile 2020 del Comitato europeo per la protezione dei dati personali (EDPB) già cit.
[72] Così, par. 3.5 (*Limitare la divulgazione di dati/l'accesso ai dati*) della Comunicazione della Commissione europea del 17 aprile 2020, cit.
[73] Così, punto 1.2. (*Sulle finalità dell'app*) del parere del Garante italiano del 1° giugno 2020, cit., p. 7.
[74] V. par. 3.5 (*Definire limiti rigorosi per la conservazione dei dati*) della Comunicazione della Commissione europea del 17 aprile 2020, cit.

le applicazioni di tracciamento il termine massimo di un mese (21 giorni di incubazione della malattia e margine di azione), l'art. 6, comma 2, lett. *e)* d.l. 28 si limita, in modo piuttosto generico, ad affermare che "i dati...siano conservati…per il periodo strettamente necessario al trattamento, la cui durata è stabilita dal Ministero della salute". Solo la lettura del parere del Garante del 1° giugno 2020 e della valutazione di impatto dello stesso del 3 giugno 2020 permette di comprendere che il Ministero della salute abbia in realtà già individuato i tempi di conservazione dei dati in relazione alle specifiche finalità e che per *Immuni* abbia già individuato un limite temporale di cancellazione ridotto rispetto a quello indicato dalla Commissione, ossia 14 giorni quanto ai dati personali memorizzati sia sui dispositivi mobili degli utenti sia nel *backend* di *Immuni*[75]. Non è chiaro però quale sia il termine iniziale di decorrenza del predetto periodo. Più correttamente, tali indicazioni sono invece già contenute all'art. 3 del *décret* 2020-650 francese, prevedendo quest'ultimo che i dati inerenti alla cronologia di prossimità registrati da *StopCovid* sul dispositivo mobile di un certo soggetto siano conservati per 15 giorni dalla loro registrazione attraverso la detta applicazione. Il medesimo termine massimo è poi previsto dall'art. 3 anche per i dati della cronologia di prossimità dei contatti a rischio di contaminazione condivisi sul *server* centrale.

Il fatto che la legislazione sia italiana, sia francese abbia previsto periodi di tempo ridotti (14 e 15 giorni) rispetto a quelli indicati dalla Commissione europea (al massimo un mese) è forse la ragione che ha indotto i predetti legislatori nazionali a non prevedere, come invece indicato nella Comunicazione del 17 aprile 2020, un lasso di tempo di conservazione più breve di un mese qualora la persona sottoposta a tampone risulti negativa[76]. Il fatto che il funzionamento stesso di *Immuni* sia connesso alla rilevata positività da Covid-19 avrebbe tuttavia dovuto indurre l'Italia (e anche la Francia) a prevedere, come suggerito dalla Commissione europea, tempi ridotti a quelli normalmente previsti nel caso in cui un soggetto allertato risulti negativo.

8. Conclusioni

L'analisi comparata svolta nei paragrafi precedenti mostra come il nostro Paese, confrontato con la difficile prova di rivedere il bilanciamento tra il diritto alla protezione dei dati personali e quello alla salute per far fronte alla pandemia Covid-19, abbia reagito in modo responsabile, mettendo la tecnologia a servizio della collettività senza pregiudicare, quantomeno in modo eccessivo o irrimediabile, i diritti fondamentali nazionali e UE. Ciò dovrebbe allora incentivare l'opinione pubblica ad

[75] In tal senso, parere del Garante italiano del 1° giugno 2020 cit., p. 3-5 e 12 e valutazione di impatto dello stesso del 3 giugno 2020, cit., pp. 5-7.
[76] In tal senso, par. 3.7 (*Definire limiti rigorosi per la conservazione dei dati*) della comunicazione della Commissione europea del 17 aprile 2020, cit.

installare *Immuni*, aumentando così la (invece piuttosto bassa) percentuale di utenti[77]. Tuttavia, soprattutto a fronte degli evidenziati vantaggi del tracciamento manuale rispetto a quello tecnologico, sarebbe stata auspicabile un'analisi più approfondita – sia ad opera del Governo e del Parlamento ma anche del Garante – dell'effettiva necessità di dotarsi di un'applicazione di tracciamento per natura particolarmente invasiva della sfera privata dei singoli. In assenza di evidenti valutazioni comparative sugli strumenti di tracciamento (manuale e tecnologico) a disposizione basate su studi scientifici, rimane allora il dubbio che il potenziamento, con operatori sanitari esperti, delle squadre di tracciamento – le quali permettono non solo un'indagine epidemiologica mirata e adeguata al caso di specie, ma anche il supporto dei soggetti potenzialmente infetti così da stabilire un rapporto di fiducia in un momento delicato – sarebbe forse potuto essere la migliore soluzione, anche in quanto più rispettosa dei diritti fondamentali nazionali e UE in gioco.

Una volta deciso poi di dotarsi di un'applicazione di tracciamento, il legislatore italiano ben avrebbe potuto adottare una normativa più dettagliata e completa che illustrasse il funzionamento – e soprattutto i limiti di funzionamento – di *Immuni*. Tale risultato era peraltro alla portata nazionale considerato che, da un lato, il GDPR e i suoi principi – necessità, proporzionalità, minimizzazione e trasparenza – delimitavano già in modo chiaro il perimetro delle iniziative nazionali, e dall'altro lato, la Commissione europea ha tempestivamente fornito indicazioni pratiche a completamento del quadro normativo generale del GDPR.

Né invero il Governo e il Parlamento italiano sembrano aver sfruttato appieno le conoscenze e i suggerimenti del Garante di cui ai pareri, particolarmente dettagliati, del 29 aprile, 1° giugno e 3 giugno 2020. L'analisi di questi ultimi mette peraltro in evidenza un dato estremamente positivo, ossia l'attiva e informata partecipazione del Garante nel corso dell'intero procedimento di adozione di *Immuni.* Come auspicato dallo stesso GDPR, esso si è così dimostrato uno degli attori principali del predetto processo normativo e dunque, più in generale, un soggetto indispensabile per ogni moderna democrazia nell'era digitale. Il suo intervento non è peraltro consistito in un mero controllo – per così dire a valle – della conformità al GDPR della legislazione interna istitutiva di applicazioni di tracciamento, ma si è sostanziato in un contributo attivo all'elaborazione dello stesso strumento normativo, ossia in un intervento per così dire a monte del procedimento. L'efficacia della loro iniziativa è allora una risposta concreta a quanti, negli anni, hanno messo in dubbio l'utilità di autorità indipendenti nel settore della tutela dei dati personali. Un'ulteriore sfida – per l'UE, gli Stati membri e i Garanti nazionali – sarà allora quella di realizzare nei prossimi mesi l'effettiva interoperabilità delle applicazioni nazionali di tracciamento, così da rispondere pienamente alle esigenze del mercato unico.

[77] Su questi aspetti v. diffusamente G. DELLA MORTE, *Quanto Immuni? Luci, ombre e penombre dell'app selezionata dal Governo italiano*, cit., spec. p. 329.

ABSTRACT: Il presente contributo è volto ad accertare la compatibilità con la legislazione UE in materia di protezione dei dati personali del d.l. 28 del 30 aprile 2020 – poi convertito nella legge 70 del 25 giugno 2020 – il quale ha permesso, per ragioni di tutela della salute pubblica al fine di contrastare la diffusione della pandemia Covid-19, l'uso in Italia di un'applicazione di tracciamento dei contatti, la c.d. Immuni, ossia di uno strumento che per natura comprime e compromette il diritto fondamentale di cui all'art. 8 della Carta dei diritti fondamentali UE.

KEYWORDS: protezione dei dati personali – Covid-19 – GDPR – tutela della salute pubblica – Immuni.

THE *IMMUNI* TRACKING APPLICATION BETWEEN NATIONAL LAW AND EU DATA PROTECTION LAW

ABSTRACT: This article aims to assess the compatibility with EU data protection law of decree law no. 28 of 30 April 2020 – converted into law no. 70 of 25 June 2020 – which allows, for reasons of public health and in order to combat the spread of the Covid-19 pandemic, the use in Italy of a contact tracing application, the so-called *Immuni* app, a tool that by nature limits and interferes with the fundamental right enshrined in art. 8 of the EU Charter of fundamental rights.

KEYWORDS: EU Data Protection Law – Covid-19 – GDPR – public health – Immuni.