ISSN 2384-9169
Fascicolo n. 3 - 2020
rivista.eurojus.it

Applicazioni di tracciamento a tutela della salute e protezione dei dati personali nell'era Covid-19: quale (nuovo) bilanciamento tra diritti?

DI SERENA CRESPI*

1. L'importanza della protezione dei dati personali e le nuove sfide dell'era Covid-19.

Negli ultimi dieci anni il diritto alla protezione dei dati personali ha acquisito sempre più importanza nel panorama giuridico nazionale, europeo e internazionale. A livello UE, esso è ormai menzionato, peraltro in modo molto dettagliato e garantendogli autonomia rispetto alla tutela della vita privata e famigliare, all'art. 8 della Carta dei diritti fondamentali UE[1], la quale dal 1° dicembre 2009 ha anche acquisito valore giuridico vincolante per ogni Istituzione europea e Stato membro in virtù dell'art. 6, par. 1 TUE[2]. A differenza poi di altri diritti fondamentali, la tutela dei dati personali, sempre nel quadro

*Professore Associato in Diritto dell'Unione europea, Università degli Studi Milano – Bicocca.

[1] Ciò segna una diversità tra la Carta UE e la CEDU ove invece la tutela dei dati personali è parte del più ampio diritto al rispetto della vita privata e familiare di cui all'art. 8 CEDU. Sull'importanza di dare autonomia al diritto alla tutela dei dati personali rispetto ad altri diritti fondamentali e, in particolare, a quello alla riservatezza della vita privata, già S. RODOTÀ, *Libertà personale. Vecchi e nuovi nemici*, in M. BOVERO (a cura di), *Quale libertà. Dizionario minimo contro i falsi liberali*, Roma-Bari, 2004, p. 33 ss., spec. p. 52. Come si avrà modo di vedere anche oltre nel presente contributo, tale diversità non impedisce tuttavia una tendenziale convergenza della giurisprudenza della due Corti almeno quanto alla tutela dei dati. In generale, auspica tale convergenza M. FRAGOLA (cur.), *La cooperazione fra Corti in Europa nella tutela dei diritti dell'uomo*, Napoli, 2012.

[2] Per un approfondimento di questi aspetti, G. STROZZI, J. RIDEAU, *La protection des droits fondamentaux dans l'Union européenne. Perspectives ouvertes par le Traité de Lisbonne*, in *Rev. aff. eur.*, 2007, p. 185 ss ; I. PINGEL, *Les références à la Charte des droits fondamentaux dans le Traité établissant une Union européenne: Mélanges en l'honneur du professeur Philippe Manin*, Paris, 2010, p. 795 ss.

successivo al trattato di Lisbona, figura anche all'art. 16 TFUE, il quale ha attribuito al legislatore UE la competenza ad adottare le norme relative alla concreta protezione delle persone fisiche con riguardo al trattamento dei dati, nonché quelle connesse alla libera circolazione degli stessi. Ed è su questa base giuridica che il 27 aprile 2016 quest'ultimo, affermando l'esigenza di modernizzare le precedenti disposizioni comuni alla luce degli sviluppi tecnologici e della globalizzazione[3], ha adottato il regolamento 2016/679 (di seguito: GDPR), che ha introdotto per la prima volta una disciplina UE orizzontale (applicabile cioè a ogni ambito giuridico-economico) e completa (relativa al settore tanto pubblico quanto privato) di tutela dei dati personali[4], nonché la direttiva 2016/680 relativa alla protezione degli stessi in materia penale[5]. Tali strumenti si aggiungono alla direttiva *e-privacy*[6] relativa al trattamento dei dati e alla tutela della vita privata nel settore delle comunicazioni elettroniche.

Come peraltro accade per gran parte dei diritti fondamentali, l'accresciuta importanza della tutela dei dati ha portato sempre più spesso la Corte di giustizia dell'Unione europea a un delicato bilanciamento del diritto in esame con altri diritti (d'autore, d'iniziativa economica, libertà d'informazione ed espressione)[7] o interessi di rilevante importanza (la lotta alla criminalità e la sicurezza nazionale)[8] coi quali esso

[3] La direttiva 95/46 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali (*GUCE* L 281/1995) e la decisione quadro 2008/977/GAI sulla protezione dei dati nel settore della cooperazione giudiziaria e di polizia in materia penale (*GUUE* L 350/2008).

[4] Sotto questo profilo, si rileva una differenza tra il sistema UE e quello di alcuni paesi extra-UE come, ad es. gli USA o la Repubblica di Singapore. Negli USA, la materia in esame è per lo più disciplinata da norme solo settoriali spesso regolamentari (*Financial Services Modernisation Act* del 1999 e *Health Insurance Portability and Accountability Act* del 1996) applicate da una pluralità di autorità differenti (*Federal Trade Commission* o l'*Office of Consumers Affairs, Department of Health*) senza il coinvolgimenti di garanti della *privacy*. Sulle differenze tra UE e USA in materia di protezione dei dati personali nonostante le salvaguardie aggiunte in via negoziale dal *Privacy Shield* del 2016, v. la recente sent. Corte di giust., 16 luglio 2016, causa C-311/18, *Data Protection Commissioner c. Facebook Ireland Ltd e Maximillian Schrems*, ECLI:EU:C:2020:559. Nella Repubblica di Singapore, la legislazione inerente alla tutela dei dati, quantomeno prima dell'emergenza sanitaria in corso, era disciplinata solo dal *Personal Data Protection Act (PDPA)* quanto al settore privato e dal *Public Sector Act (PSGA)* quanto a quello pubblico. In dottrina, sulle differenze tra sistema UE e USA, P. DE HERT, S. GUTWIRTH, R. LEENES (eds), *Reloading Data Protection. Multidisciplinary Insights and Contemporary Challenges*, Dordrecht, Heidelberg, London, New York, 2014. Quanto al sistema di Singapore, J. BAY, J. KEK, A. TAN, C. SHENG HAU, L. YONGQUAN, J. TAN, T. ANH QUY (*Government Technology Agency)*, *BlueTrace: A privacy-preserving protocol for community-driven contact tracing across borders*, https://bluetrace.io/static/bluetrace_whitepaper-938063656596c104632def383eb33b3c.pdf.

[5] Tali atti UE sono rispettivamente pubblicati in *GUUE* L 119/1 e L 119/89 entrambi del 2016. In generale, sulla riforma del sistema UE di tutela dei dati del 2016, E. DEGRAVE, *La protection des données à caractère personnel enfin reformée*, in *Jour. dr. eur*., 2016, p. 136 ss.; M. CORRALES, M. FENWICK, N. FORGÒ (eds), *New Technology, Big Data and the Law*, ed. 1, Singapore, 2017, p. 46 ss.

[6] Direttiva 2002/58 del Parlamento europeo e del Consiglio del 12 luglio 2002, *GUUE* L 201/2002. Il presente contributo ha scelto di concentrare l'analisi di compatibilità delle legislazioni nazionali inerenti le applicazioni di tracciamento con il GDPR, limitandosi a brevi cenni sulla direttiva qui in nota.

[7] Così in Corte giust., 13 maggio 2014, causa C-131/12, *Google Spain*, ECLI:EU:C:2014:317. In dottrina, *ex multiis*, S. CRESPI, *Diritti fondamentali, Corte di giustizia e riforma del sistema UE di protezione dei dati personali*, in *Riv. it. dir. pubbl. com.*, 2015, 819 ss.; C. KUNER, Google Spain *in the EU and international context*, in *Maastricht jour. eur. comp. law*, 2015, 158 ss.

[8] In tal senso, Corte giust., 8 aprile 2014, cause C-293/12 e C-594/12, *Digital Rights Ireland*, ECLI:EU:C:2014:238; 6 ottobre 2015, causa C-362/14, *Schrems I*, ECLI:EU:C:2015:650; 21 dicembre

entrasse in conflitto, in taluni casi per ridurne l'ampiezza attuativa e in altri casi invece per estenderne l'ambito d'applicazione. Lo stesso GDPR è proprio il risultato legislativo di un siffatto contemperamento tra diritti (libertà d'espressione e di informazione di cui all'art. 85 GDPR, diritto d'accesso ai documenti di cui agli artt. 15 e 86 GDPR) e interessi (libera circolazione dei dati di cui agli artt. 1 e 51 GDPR, ricerca scientifica di cui all'art. 89 GDPR)[9].

L'assetto così come costruito dal GDPR anche alla luce della giurisprudenza UE è stato di recente messo sotto pressione dalla pandemia Covid-19, la quale ha confrontato i sistemi giuridici nazionali, UE e internazionali a doversi interrogare – ed eventualmente riesaminare – il bilanciamento tra diritti fondamentali – e tra questi di quello alla protezione dei dati – alla luce della sopraggiunta esigenza di tutela della salute[10]. La lotta al Covid-19 implica in effetti, tra l'altro, la raccolta, l'uso e il trasferimento di dati medici dei pazienti – ossia di una categoria di dati personali particolarmente sensibile – al fine di ricostruire la mappa epidemiologica del contagio, nonché potrebbe comportare la geo-localizzazione tramite le moderne tecnologie dei soggetti infetti per evitare o addirittura sanzionare spostamenti fuori dal domicilio ove essi siano confinati o l'uso di taluni dati per risalire agli individui entrati in contatto con il virus. Come rilevato – seppur con una certa cautela – dalla Commissione europea e dal Centro europeo per la prevenzione e il controllo delle malattie (ECDC)[11], le applicazioni mobili, comprese quelle con funzionalità di tracciamento, sono anche particolarmente importanti in fase di revoca delle misure di contenimento, quando cioè il rischio di infezione cresce man mano che aumenta la contiguità tra gli individui.

2016, cause C-203/15 e 698/15, *Tele2 Severige e Watson*, ECLI:EU:C:2016:970, nonché le concl. avv. gen Sanchez-Bordona, 15 gennaio 2020, cause C-511/18 e 512/18, *La Qauadrature du Net*; ECLI:EU:C:2020:6; causa C-623/17, *Privacy International*, ECLI:EU:C:2020:5; causa C-520/18, *Ordre des barreaux francophones et germanophones*, ECLI:EU:C:2020:7. V. in merito anche la recente sent. Corte di giust., 16 luglio 2016, *Data Protection Commissioner (Schrems II)* cit. Per un quadro di insieme di tutte le sentt. precit. mi permetto di rinviare a SERENA CRESPI, *Il trasferimento dei dati personali UE in Stati terzi: dall'Approdo sicuro allo Scudo UE/USA per la* privacy, in *Dir. pub. comp. eur.*, 2016, p. 687 ss.; ID., *Sicurezza nazionale e diritti fondamentali alla luce della giurisprudenza UE in materia di tutela dei dati personali*, in *Riv. it. dir. pub. com.*, 2017, 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 integr. 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.

[9] Sulla disciplina del GDPR, M. BOTTINO, *Approvato il nuovo regolamento generale per la protezione dei dati personali nell'UE*, in *Eurojus*, 26 aprile 2016. Per l'analisi delle single disposizioni del GDPR, C. KUNER, L.A. BYGRAVE, C. DOCKSEY (ed.), *The EU General Data Protection Regulation (GDPR). A Commentary*, Oxford, 2020.

[10] In generale sulle le iniziative UE nel periodo Covid-19, G. DI FEDERICO, *Stuck in the middle with you…wondering what it is I should do. Some considerations on EU's response to COVID-19*, in *Eurojus*, n. 3, 2020, p. 60 ss., nonché il numero speciale della medesima Rivista, *L'emergenza sanitaria Covid-19 e il diritto dell'Unione europea. La crisi, la cura, le prospettive*.

[11] Comunicazione della Commissione europea 17 aprile 2020, *Orientamenti sulle app a sostegno della lotta alla pandemia di covid-19 relativamente alla protezione dei dati*, *GUUE* C 124 I/1, https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52020XC0417(08)&from=IT, spec. par. 1 (*Contesto*). Quanto al ECDC, *Contact tracing for COVID-19: current evidence, options for scale-up and an assessment of resources needed* (www.ecdc.europa.eu/sites/default/files/documents/COVID-19-Contract-tracing-scale-up.pdf.), aprile 2020, spec. p. 2.

In tale contesto, pare allora utile chiedersi se, ed eventualmente in quale misura, sia possibile coniugare il rispetto del diritto alla tutela dei dati personali con un'efficace lotta all'espansione della pandemia mediante l'uso, ad esempio, di applicazioni di tracciamento che, avendo come finalità quella d'individuare e poi di allertare i soggetti entrati in contatto con il Covid-19, comportano per natura significative compressioni al diritto di cui all'art. 8 della Carta e alla disciplina positiva dello stesso contenuta nel GDPR. La ricostruzione del quadro giuridico complessivo permetterà poi di apprezzare le scelte operate fino ad ora almeno da taluni Stati membri – principalmente l'Italia e la Francia che, al momento in cui si scrive, dispongono di applicazioni di tracciamento pienamente operative e di una legislazione sottesa consultabile, ma anche il Belgio e Olanda, ove l'adozione dei predetti strumenti, pur ancora *in fieri*, è stata oggetto di particolare attenzione da parte dei garanti nazionali e della società civile[12] – quali indicatori dell'attitudine di un certo sistema nazionale verso la tutela dei diritti fondamentali.

Ciò vale peraltro anche per Stati terzi adeguati ai sensi dell'art. 45 GDPR – ossia Andorra, Argentina, Canada, isole Faeroe, Guernsey, Israele, isola di Man, Jersey, Svizzera, Nuova Zelanda, Giappone e Uruguay – o che ambiscono a questa adeguatezza – ad esempio, la Corea del Sud[13]. Pur se tali aspetti non potranno essere affronti nel dettaglio nel presente contributo, la decisione di adeguatezza UE richiede, infatti, una valutazione olistica del sistema giuridico del paese terzo che va oltre l'esame della sola legislazione sulla protezione dei dati, guardando peraltro anche la prassi, e che potrebbe dunque anche interessarsi alle misure di raccolta di dati adottate nell'ambito della lotta contro la pandemia. Posto poi che l'adeguatezza di un sistema agli standard europei deve essere periodicamente rivalutata dalla Commissione europea (art. 46, par. 3, GDPR), è sempre possibile che l'adozione di misure Covid-19 contrarie allo spirito UE possano condurre in futuro alla perdita dello *status* di paese adeguato, a maggior ragione dopo la conferma della Corte di giustizia nella recente sentenza *Schrems II* del severo test della sostanziale equivalenza tra sistemi UE ed extra-UE.[14]

2. Applicazioni nazionali di tracciamento e protezione UE dei dati: i confini dell'azione interna e dell'UE alla luce dei principi di necessità e proporzionalità.

[12] In aggiunta a tali paesi membri saranno in realtà prese in esame le iniziative anche di altri Stati UE ed extra-UE ove e nella misura in cui esse risultino – così da essere valutate – da documenti ufficiali consultabili o siano stati dibattuti dell'accademia nazionale.

[13] Tali paesi e territori beneficiano di una decisione di adeguatezza adottata dalla Commissione europea. L'effetto di tale decisione è consentire la libera circolazione dei dati personali verso il paese terzo in questione senza che l'esportatore dei dati debba fornire ulteriori garanzie o ottenere un'autorizzazione. Quanto ai negoziati per l'adeguatezza UE della Corea del Sud, v. comunicato stampa del 30 giugno 2020 del Consiglio europeo, *Joint press release: Republic of Korea - EU Leaders' video conference meeting*, spec. par. 11,www.consilium.europa.eu/it/press/press-releases/2020/06/30/joint-press-release-republic-of-korea-eu-leaders-video-conference-meeting.

[14] Su adeguatezza UE e Covid-19, C. DOCKSEY, C. KUNER, *The Coronavirus Crisis and EU Adequacy Decisions for Data Transfers*, 3 aprile 2020, https://europeanlawblog.eu/2020/04/03/the-coronavirus-crisis-and-eu-adequacy-decisions-for-data-transfers.

In modo lungimirante il GDPR, come già ricordato, non si limita solo a disciplinare l'esercizio del diritto alla protezione dei dati ma bilancia quest'ultimo con altri diritti e interessi coi quali il primo entri o possa entrare in conflitto. Per quanto riguarda la tutela della salute, il GDPR prevede rispettivamente all'art. 9, par. 2, let. *i)* e al considerando 46 che il trattamento di dati personali 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 loro diffusione»[15]. Tale bilanciamento si riflette anche all'art. 23, par. 1, let. *e*) GDPR che stabilisce che il diritto UE o dello Stato membro cui è soggetto il responsabile del trattamento può limitare, mediante misure legislative ed entro certi determinati confini, la portata (solo) di taluni obblighi e diritti (quelli di cui agli artt. da 12 a 22 e l'art. 34 GDPR) «per salvaguardare importanti obiettivi di interesse pubblico generale UE o di uno Stato membro in materia *di sanità pubblica*»[16]. E' dunque lo stesso GDPR ad ammettere – quando ancora l'idea di un'emergenza sanitaria in Europa sembrava piuttosto teorica – una compressione del diritto previsto all'art. 8 della Carta disciplinato del GDPR oltre ciò che è normalmente consentito allorché si tratti di proteggere il diritto, parimenti essenziale, della salute. In altri termini, la legislazione UE non solo non ostacola l'uso di strumenti tecnologici che, come le applicazioni di tracciamento, possono favorire il contenimento di emergenze sanitarie, ma anzi ne consente proprio l'adozione, pur se circoscrivendone l'ambito d'attuazione entro taluni confini.

La questione da indagare non è allora se, in virtù del GDPR, sia possibile impiegare strumenti di tracciamento, ma a quali condizioni essi possano essere usati negli Stati membri e, in virtù dell'art. 45 GDPR, anche in paesi terzi che vogliano mantenere o acquisire lo *status* di adeguatezza UE. Il considerando 46 e gli artt. 6, 9 e 23 GDPR non sono, infatti, un salvacondotto che permette agli Stati membri o terzi d'invocare la tutela della salute pubblica per giustificare l'adozione di qualsiasi misura derogatoria al diritto della protezione dei dati e alla disciplina (e alle conquiste) del GDPR. E' lo stesso art. 9 GDPR, letto insieme all'art. 6 e al considerando 46, a stabilire le condizioni che permettono il trattamento di dati relativi alla salute in deroga al generale divieto di trattamento dei cosiddetti dati sensibili, prevendendo in particolare che tale trattamento sia consentito (i) se necessario per motivi di sanità pubblica e (ii) se fondato su normative nazionali che contengano misure appropriate e specifiche per tutelare i diritti dell'interessato. Parimenti, è l'art. 23 GDPR, anche alla luce del considerando 73, che precisa le limitazioni che la legislazione UE o quella nazionale possono apportare alla disciplina comune per ragioni di sanità pubblica, circoscrivendo tale possibilità solo a taluni obblighi e diritti GDPR – alle modalità per l'esercizio dei diritti dell'interessato di cui agli artt. 13-22 GDPR (art. 12); accesso alle informazioni raccolte dal titolare del trattamento (artt. 13-15), alla rettifica (art. 16) e/o la cancellazione dei dati raccolti (art. 17), nonché in alcuni casi la limitazione del trattamento degli stessi (art. 18); diritto alla

[15] Il considerando 46 si riferisce all'art. 6 GDPR che disciplina la liceità del trattamento dei dati.
[16] Corsivo aggiunto dall'autore.

portabilità dei dati (art. 20), di opposizione (art. 21) e di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato (art. 22); 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 di comunicare una violazione dei dati (art. 34) – e stabilendo che tali limitazioni in ogni caso «devono rispettare l'essenza dei diritti e delle libertà fondamentali della Carta e della CEDU in una società democratica ed essere necessarie e proporzionate». La previsione di tali condizioni, in termini sia di liceità del trattamento (artt. 6 e 9) che di possibili limitazioni a taluni obblighi e diritti stabiliti dal GDPR (art. 23), conferma allora *a contrario* che il GDPR resti pienamente applicabile anche quando si tratti di adottare legislazioni interne motivate da ragioni di sanità pubblica, potendo la sua attuazione essere limitata per tali ragioni esclusivamente in ambiti circoscritti (artt. 12-22 e 34 GDPR) e solo ove realmente necessario e in ogni caso in modo proporzionato[17]. Il fatto poi che gli artt. 9 e 23 GDPR siano norme derogatorie suggerisce l'applicazione di questi ultimi anche solo per farvi ricorso e dunque per l'adozione stessa di legislazioni nazionali istitutive di applicazioni di tracciamento motivate dall'esigenza di tutelare la salute pubblica.

L'applicazione dei principi di necessità e proporzionalità nell'ambito in esame, già prescritta dall'art. 9 e 23 GDPR, sarebbe stata in ogni caso possibile in virtù della sola giurisprudenza UE. Negli ultimi anni, la Corte ha, infatti, ripetutamente confermato l'applicazione degli stessi per valutare la compatibilità di misure interne adottate in settori di competenza nazionale (per lottare contro la criminalità o per esigenza di sicurezza interna)[18] entrate in tensione con il diritto di cui all'art. 8 della Carta. Come già ricordato dai giudici di Lussemburgo nella pronuncia *Schrems I*, un accesso generalizzato – e dunque per definizione non necessario né proporzionato – ai dati di cittadini UE ad opera di autorità pubbliche o imprese, essendo lesivo dell'essenza del diritto fondamentale alla tutela dei dati personali, non può essere mai giustificato, prevedendo l'art. 52, par. 1, della Carta che eventuali limitazioni all'esercizio dei diritti devono sempre rispettare il contenuto essenziale di detti diritti e libertà. Come spesso accade nel sistema UE, le limitazioni stabilite all'art. 9 e 23 GDPR codificano così a livello positivo principi già

[17] Così, anche l'EDPB, *Statement on restrictions on data subject rights in connection to the state of emergency in Member States,* https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_art_23gdpr_20200602_en.pdf, 2 giugno 2020, 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*, Vol. 1, Issue 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*, 22/2018, p. 1 ss.

[18] Così, Corte giust., *Digital Rights Ireland* cit. e *Tele2* cit. quanto a misure interne adottate per lottare contro la criminalità; *Schrems* I cit., punti 87-94, e Schrems II cit. quanto a misure interne motivate dall'esigenza di garantire la sicurezza nazionale; nonché il parere Corte giust., 26 luglio 2017, C-592/17, 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.

elaborati dalla Corte di giustizia. Se allora tutto ciò è vero, gli Stati membri sono dunque competenti ad adottare provvedimenti relativi ad applicazioni di tracciamento per lottare la diffusione del Covid-19, ma questa libertà incontra un limite nel rispetto del GDPR e dei principi di necessità e proporzionalità, i quali intervengono per evitare l'abuso di questo potere, l'irrimediabile pregiudizio di diritti fondamentali condivisi, nonché per favorire la coerenza del sistema comune. In altri termini, al fine di garantire il rispetto del diritto vincolante UE in materia di tutela dei dati personali, le legislazioni nazionali istitutive di tali applicazioni dovranno, in positivo, prevedere opportune salvaguardie che garantiscano una proporzionata compressione del diritto alla tutela dei dati motivata dall'esigenza di proteggere la salute nel particolare contesto di una pandemia.

Né invero una tesi diversa potrebbe essere sostenuta rivendicando la piena competenza nazionale in materia di salute, disponendo in tale settore l'Unione solo di un mero potere di coordinamento e sostegno delle singole iniziative nazionali di cui agli artt. 6 e 168 TFUE e alla dichiarazione 32 relativa all'art. 168, par. 4, let. *c)*[19]. Come già ricordato, la disciplina GDPR è orizzontale e si applica così a ogni trattamento di dati, non variando in funzione delle competenze UE o nazionali in una certa materia. 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 dell'Unione in situazioni ricadenti nell'ambito di applicazione di quest'ultimo[20], dovendo anche in tal caso le legislazioni interne tener conto – e dunque rispettare – le regole comuni con le quali le prime entrino in contatto e in conflitto, pena il pregiudizio del buon funzionamento del sistema comune di cui i paesi membri hanno scelto di far parte. Se ciò vale per ambiti di competenza nazionale esclusiva neppure menzionati nei trattati, questo principio generale di funzionamento dei rapporti tra diritto UE e interno si applica allora anche a un ambito come quello in esame (salute) che riconosce all'Unione un certo potere (di sostengo e coordinamento delle azioni degli Stati membri). E in effetti

[19] In realtà, anche alla luce degli artt. 4, par. 2, lett. k, TFUE (competenza concorrente tra UE e Stati membri da esercitarsi in virtù del principio di sussidiarietà di cui all'art. 5 TUE e al Protocollo 2 quanto ai «problemi comuni di sicurezza in materia di sanità pubblica, per quanto riguarda gli aspetti definiti nel presente trattato»), 9 TFUE (che menziona la salute umana tra le esigenze che devono guidare la definizione e l'attuazione delle politiche e azioni comuni) e 35 della Carta dei diritti fondamentali («ogni persona ha il diritto di accedere alla prevenzione sanitaria e ad ottenere cure mediche adeguate») e il quadro giuridico UE nel settore della salute pubblica è più articolato e la delimitazione esatta tra competenze UE e degli Stati membri non è sempre un'operazione semplice. In tal senso anche, P. DE PASQUALE, *Le competenze dell'Unione europea in materia di sanità pubblica e la pandemia di Covid-19*, in *Saggi – DPCE online*, 2020/2, p. 2295 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 ss.; F. BESTAGNO, *La tutela della salute tra competenze dell'Unione europea e degli Stati membri*, in *Studi sull'integrazione europea*, 2, 2017, p. 317 ss.

[20] Così, *ex multiis*, Corte giust., 24 novembre 1998, causa C-274/96, *Bickel e Franz*, ECLI:EU:C:1998:563, punto 17 in materia penale; 2 ottobre 2003, causa C-148/02, *Garcia Avello*, ECLI:EU:C:2003:539, punto 25 sul nome delle persone; 12 luglio 2005, causa C-403/03, *Schempp*, ECLI:EU:C:2005:446, punto 19 in materia di fiscalità diretta, 12 settembre 2006, causa C-145/04, *Spagna c. Regno Unito*, ECLI:EU:C:2006:543, punto 78 riguardo al diritto di elettorato alle elezioni del PE; 2 marzo 2010, causa C-135/08, *Rottmann*, 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[21].

Tali considerazioni inducono peraltro a una riflessione ulteriore. Se le legislazioni nazionali istitutive di applicazioni di tracciamento devono rispettare il diritto UE alla protezione dei dati, gli Stati membri, in luogo di moltiplicare gli sforzi unilaterali per elaborare strumenti di tal genere, avrebbero potuto cercare una strada alternativa (e una base giuridica innovativa) per adottare un'unica applicazione di tracciamento. Valorizzando, ad esempio, il fatto che quest'ultima sia solo uno strumento a sostengo della politica interna di contrasto all'emergenza sanitaria, si sarebbe forse potuto tentare di impiegare il par. 5 dell'art. 168 TFUE, che prevede l'uso della procedura legislativa ordinaria e la consultazione del Comitato economico e sociale e del Comitato delle Regioni per adottare «misure volte a lottare contro i grandi flagelli che si propagano oltre frontiera e contro gravi minacce per la salute a carattere transfrontaliero». Seppur un po' forzatamente, riprendendo il modello di decisione UE istitutiva del meccanismo europeo di coordinamento delle protezioni civili degli Stati membri – parimenti materia di competenza UE di sostengo e coordinamento[22] – tale legislazione UE, in quanto volta solo a introdurre nei paesi membri un mero strumento tecnico di tracciamento dei contatti nell'UE, avrebbe forse potuto non violare il divieto di armonizzare le disposizioni, legislative e regolamentari, interne di cui alla medesima norma, le quali, usando tale base giuridica, non sarebbero neppure esistite.

Considerata poi l'abitudine dei cittadini UE di circolare, anche per ragioni di turismo, oltre i confini nazionali, la capacità esclusivamente interna delle applicazioni in esame obbliga coloro che, a seguito della (ormai di nuovo, tendenzialmente, piena) libera circolazione delle persone[23], intendano spostarsi in paesi limitrofi a moltiplicare l'installazione di applicazioni analoghe, il che ben potrebbe disincentivarli dal circolare nel mercato unico o dal dotarsi anche solo di uno di questi strumenti[24]. Il divieto d'armonizzazione delle normative nazionali in materia di sanità di cui all'art. 168 TFUE avrebbe allora potuto essere aggirata – come peraltro già fatto in passato – grazie all'adozione di misure sul ravvicinamento delle disposizioni nazionali relative

[21] In tal senso, Corte giust. 16 maggio 2006, causa C-372/04, *Yvonne Watts contro Bedford Primary Care Trust e Secretary of State for Health*, ECLI:EU:C:2006:325, punto 92; nonché la precedente Corte giust. 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, punti 44-46.

[22] Un intervento di questo genere sembra richiamare l'utilizzo della competenza parimenti di sostengo di cui all'art. 6 TFUE in materia di protezione civile quanto alla creazione del c.d. Meccanismo unionale di protezione civile. Su tale aspetto, già S. CRESPI, *Commento all'art. 196 TFUE*, in F. POCAR, M.C. BARUFFI (a cura di), *Commentario breve ai trattati dell'Unione europea*, Milano, 2014.

[23] Sulla chiusura delle frontiere nel periodo Covid-19, G. CAGGIANO, *Competenze dell'Unione, libertà di circolazione e diritti umani in materia di controlli delle frontiere, misure restrittive della mobilità e protezione internazionale*, https://www.aisdue.eu; nonché S. MONTALDO, *The COVID-19 Emergency and the Reintroduction of Internal Border Controls in the Schengen Area: Never Let a Serious Crisis Go to Waste*, in *European Papers*, 25 aprile 2020, p. 1 ss.

[24] In tal senso, già C. FIORILLO, *La protezione dei dati personali nel diritto UE di fronte all'emergenza del COVID-19*, nel numero speciale di *Eurojus* già cit., p. 63 ss., spec. p. 72.

al funzionamento del mercato interno di cui all'art. 114 TFUE[25]. L'importanza di questi aspetti è testimoniata dal fatto che, proprio a fronte delle iniziative solo unilaterali degli Stati membri, la Commissione europea[26] e il Comitato europeo per la protezione dei dati (di seguito: EDPB)[27] stanno lavorando al fine di rendere il prima possibile interoperative le predette applicazioni. Come si avrà modo di vedere meglio in seguito, prime indicazioni in tal senso sono state adottate il 16 giugno 2020 sia dall'EDPB sia dalla Commissione europea[28].

3. *Segue*: Applicazioni di tracciamento e la fiducia dei cittadini UE.

La previsione nelle leggi di adozione di applicazioni di tracciamento di garanzie adeguate, necessarie e proporzionate, è poi ancora più essenziale almeno per un duplice ordine di ragioni. Innanzitutto, perché tali strumenti possono comprimere e per tale via compromettere anche diritti fondamentali diversi da quello della protezione dei dati come la libertà di circolazione, il diritto d'impresa, d'associazione e riunione, nonché di espressione, di opinione e la libertà di religione[29]. Identificare l'associazione politica o religiosa frequentata da un certo soggetto tracciato per finalità di contrasto della pandemia può in effetti rilevare le preferenze politiche o le scelte religiose dello stesso. L'uso dei dati raccolti attraverso un'applicazione di tracciamento per finalità ulteriori a quelle che ne hanno ispirato la raccolta – tutela della salute e lotta a un'emergenza sanitaria – aumenta così il rischio di discriminazioni, stigmatizzazioni o ineguaglianze.

---

[25] Sull'esigenza di valorizzare l'uso dell'art. 114 TFUE anche G. CAGGIANO, *Competenze dell'Unione* cit., spec. p. 82. Esclude invece del tutto la possibilità di avere una base giuridica utile, P. DE PASQUALE, *Le competenze dell'Unione europea in materia di sanità pubblica* cit., spec. p. 2298.

[26] 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 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.

[27] Quanto al EDPB, *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.

[28] V. *Interoperability guidelines for approved contact tracing mobile applications in the EU* adottate dall'*eHealth network* il 13 maggio 2020, 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 iugno 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.

[29] In tal senso, par 3 (*Elementi per un uso fiduciario e responsabile delle app*) della Comunicazione della Commissione europea del 17 aprile 2020 cit., nonché il *Report* dell'agenzia europea FRA, *Coronavirus Pandemic in the EU – Fundamental Rights Implications: with a Focus on Contact-Tracing Apps*, aprile 2020, spec. p. 41, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-coronavirus-pandemic-eu-bulletin-may_en.pdf.

Pur se le indicazioni fornite della Commissione europea nella sua comunicazione del 17 aprile 2020 quanto alle caratteristiche che le applicazioni, tra l'altro, di tracciamento devono possedere per rispettare la legislazione UE in materia di protezione dei dati hanno comprensibilmente un ambito d'attuazione circoscritto solo al diritto di cui all'art. 8 della Carta, talune regole ivi previste – le limitazioni del tipo di dati raccolti, della durata della loro conservazione o delle finalità d'uso degli stessi in virtù dei principi di minimizzazione, *privacy by design* e *privacy by default*[30]– costituiscono in ogni caso un argine avverso condotte abusive anche per tali ulteriori diritti.

In secondo luogo, in un sistema come quale UE ove, in linea di principio, non potrebbe sussistere l'obbligo d'installare applicazioni di tracciamento, l'efficacia delle stesse varia in base al numero di individui che volontariamente scelgono di impiegarla – secondo uno studio dell'Università di *Oxford*, almeno il 60% dei cittadini di un certo Stato[31] – il che a propria volta dipende dalla fiducia riposta dagli stessi nello strumento in esame[32]. Da analisi statistiche compiute non solo dalla Commissione europea ma anche da imprese nell'ultimo biennio – a seguito cioè dell'effettiva applicazione del GDPR negli ordinamenti giuridici nazionali – risulta che i consumatori anche europei attribuiscano sempre più importanza alla protezione dei dati. Un'indagine pubblicata a dicembre 2019 dalla multinazionale CISCO compiuta su un campione di 2.600 adulti di Stati UE, di Asia e Nord America di diversa età, sesso e livello socio-economico, ha rilevato che ben l'84% degli intervistati ritiene la tutela dei dati una priorità, auspicandone un maggior controllo sul modo in cui essi sono usati sia dalle imprese sia dagli Stati[33]. Di questi, l'80% ha poi precisato di voler agire o di aver già agito, modificando le proprie *privacy preferences* nell'uso di servizi *online*, per proteggere i propri dati, giungendo in taluni casi fino a cambiare operatore o fornitore in ragione delle troppo vaghe politiche di *privacy* o di eccessiva condivisione dei dati con terzi e dunque per ragioni diverse da quelle per i quali il consumatore aveva fornito i propri dati. Il modo in cui questi ultimi sono gestititi è, in altri termini, sempre più considerato un indicatore del modo cui una società tratta i consumatori e dunque un fattore in grado di orientare le decisioni di acquisto. Non sorprende allora che, sempre secondo tale sondaggio, una percentuale variabile dal 36 % al 47% degli intervistati (variabile in funzione del prodotto offerto e del beneficio tratto) affermi di provare una sensazione di disagio circa l'uso di beni o servizi offerti a prezzo ridotto qualora il consumatore scelga di condividere parte dei propri dati (localizzazione) o informazioni personali (sulla propria casa o sulla propria autovettura).

---

[30] I principi *privacy by design* e *privacy by default* – ossia di finalità, trasparenza, sicurezza, proporzionalità, pertinenza e minimizzazione dei dati raccolti, nonché durata della conservazione – sono contenuti all'art. 25 GDPR.

[31] UNIVERSITY OF OXFORD, *Digital contact-tracing can slow or even stop coronavirus transmission and ease us put of lockdown*, 16 April 2020, 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.

[32] Così, par 3 (*Elementi per un uso fiduciario e responsabile delle app*) della Comunicazione della Commissione europea del 17 aprile 2020 cit.

[33] CISCO, *Consumer Privacy Survey. The growing imperative of getting data privacy right*, www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-series-2019-cps.pdf.

Ora, pur se, come qualsiasi statistica, anche quella appena richiamata debba essere considerata con una certa cautela, i dati evidenziati – peraltro confermati dalla stessa Commissione europea[34] – esprimono quantomeno una tendenza di fondo, ossia quella di una maggior consapevolezza dei consumatori dell'importanza della tutela dei propri dati personali immessi in Internet. A fronte di ciò, l'efficacia di applicazioni di tracciamento a installazione volontaria, la quale è connaturata al numero di utilizzatori e alla fiducia riposta in esse dall'opinione pubblica, sarà allora tanto maggiore quanto lo strumento adottato sia in grado, nel raggiungere l'obiettivo primario di contrasto dell'epidemia, di tutelare i dati personali nei confronti di imprese e Stati. La previsione di necessarie, proporzionate e trasparenti salvaguardie potrebbe allora essere proprio la chiave di volta per massimizzare l'uso e l'efficacia degli strumenti in esame.

4. Salvaguardie comuni ispirate ai criteri di necessità e proporzionalità: gli orientamenti della Commissione europea.

Per garantire un approccio coerente in tutta l'Unione e fornire indicazioni agli Stati membri e agli sviluppatori di applicazioni di tracciamento, la Commissione europea ha presentato – con la raccomandazione dell'8 aprile 2020 e la successiva comunicazione del 17 aprile 2020 – una serie di indicazioni circa i requisiti che questi strumenti devono possedere per garantire il rispetto del diritto dell'Unione e in particolare del GDPR, come abbiamo visto pienamente applicabile anche alla luce dei principi di necessità e proporzionalità così come interpretati dalla Corte di giustizia. Sebbene le indicazioni della Commissione non siano per loro natura vincolanti, il rispetto delle stesse limita l'intrusività delle applicazioni di tracciamento e, traducendo in termini concreti le regole vincolanti del GDPR e della pertinente giurisprudenza UE, ne garantisce la conformità con il diritto comune, evitando di esporre i paesi membri a procedure di infrazione o rinvii pregiudiziali, nonché rafforzando quella fiducia dei cittadini che, come già osservato, è alla base del successo delle applicazioni di tracciamento.

Le indicazioni contenute nella comunicazione della Commissione europea sono state peraltro riprese e per tale via confermate nelle di poco successive linee guida n. 04/2020 del 21 aprile 2020 del EDPB[35], nonché nel *Joint Statement* del 28 aprile 2020 del Consiglio d'Europa quanto alla conformità di applicazioni di tracciamento con le Convenzioni 108 e 108+ sulla protezione dei dati personali[36]. Ciò conferma peraltro la più volte rilevata convergenza tra Corti CEDU e UE quantomeno su questioni inerenti

[34] In tal senso, Comunicazione della Commissione europea del 24 giugno 2020, *La protezione dei dati come pilastro dell'autonomia dei cittadini e dell'approccio dell'UE alla transizione digitale: due anni di applicazione del regolamento generale sulla protezione dei dati*, spec. par. 1, https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52020DC0264&from=EN.

[35] EDPB, *Sull'uso dei dati di localizzazione e degli strumenti per il tracciamento dei contatti nel contesto dell'emergenza legata al COVID-19*, https://edpb.europa.eu/our-work-tools/our-documents/linee-guida/guidelines-042020-use-location-data-and-contact-tracing_it.

[36] Il *Joint Statement* è reperibile https://rm.coe.int/covid19-joint-statement-28-april/16809e3fd7.

alla tutela dei dati[37], la quale è così importante in vista della sempre possibile futura adesione dell'UE alla CEDU prescritta all'art. 6 TUE[38].

Il tempestivo intervento della Commissione europea è probabilmente da ricondurre al fatto che, in vista della fase di de-confinamento prevista per giugno/luglio 2020, ben venti Stati membri – Austria, Bulgaria, Belgio, Cipro, Croazia, Danimarca, Estonia, Finlandia, Francia, Germania, Irlanda, Italia, Lettonia, Lituania, Portogallo, Polonia, Spagna, Slovacchia e Repubblica ceca – prendendo esempio dall'esperienza di paesi asiatici come Singapore o Corea del Sud, avevano avviato già a marzo 2020 unilaterali riflessioni circa l'adozione di applicazioni di tracciamento[39]. Almeno a giugno 2020, questi strumenti sono ormai operativi in Austria[40], Bulgaria[41], Cipro[42],

[37] La sent. Corte giust. *Tele2* cit. si rifà alle sentt. CEDU 15 dicembre 2015, 47143/06, *Zakharov c. Russia*, e 12 gennaio 2016, 37138/14, *Szabò e Vssy c. Ungheria*. La sent. CEDU *Zahkarov* cit. cita le sentt. Corte giust. *Digital Rights Ireland*, e *Tele2*. La Corte di Strasburgo e quella di Lussemburgo sono così sostanzialmente allineate quanto alla necessità di sottoporre il trattamento dei dati personali da parte delle autorità pubbliche per motivi di lotta alla criminalità (*Digital Rights Ireland* e *Tele2*) e, in particolare, di quelle di *intelligence* per ragioni di sicurezza nazionale (*Schrems*, *Tele2*, *Zakharov* e *Szabò e Vissy*) a condizioni e limiti analoghi, ispirati al principio di necessità e di proporzionalità.

[38] Sulla volontà di riprendere i negoziati per l'adesione dell'UE alla CEDU (avviata con lettera del 31 ottobre 2019 del Presidente e del vice-Presidente della Commissione europea al Segretariato generale CEDU), interrotti a seguito del parere negativo della Corte di giustizia 2/13, v. il rapporto sulla riunione informale del 25 giugno 2020 tra i rappresentati UE e CEDU, https://rm.coe.int/cddh-47-1-2020-rinf-fr/16809efedc.

[39] Per un'analisi dei sistemi nazionali quanto all'adozione di applicazioni di tracciamento, v. il *Report* dell'agenzia europea FRA di aprile 2020 cit., pp. 48-52, nonché i siti web del Dipartimento *Law, Science, Technology and Society* dell'Università VUB di Bruxelles, https://lsts.research.vub.be/en/data-driven-approaches-to-covid-19-data-protection-law-dpl-x-covid-19, o del *Future of Privacy Forum*, https://fpf.org/2020/04/30/european-unions-data-based-policy-against-the-pandemic-explained/. Il Report della FRA di aprile 2020 è stato poi aggiornato con i successivi Report del 31 maggio e 30 giugno 2020, reperibili sul sito dell'agenzia.

[40] L'Austria è stato il primo paese membro a introdurre un'applicazione di tracciamento già il 25 marzo 2020, la c.d. *Corona App*. In tal senso, 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.

[41] Sull'app *VirusSafe* bulgara di aprile 2020, *Report* dell'agenzia europea FRA di aprile 2020 cit., p. 48 e il sito web www.euractiv.com/section/digital/news/covid-19-mobile-app-available-to-governments-for-a-symbolic-euro.

[42] Sull'applicazione di tracciamento cipriota *CovTrace*, *Report* dell'agenzia europea FRA di aprile 2020 cit., p. 48 e https://covid-19.rise.org.cy/RISE_CovTracer_Privacy_Policy_EN.pdf.

Italia[43], Francia[44], Polonia[45], Slovacchia[46] e Repubblica ceca[47]. Sono invece a uno stadio avanzato di elaborazione le applicazioni di tracciamento di Belgio, Irlanda, Paesi Bassi, Danimarca, Estonia, Lituania, Germania, Spagna e Finlandia. Solo sei paesi – Grecia, Lussemburgo, Romania, Malta, Slovenia, Svezia e Ungheria – sembrano ancora oggi orientati ad escluderne l'uso[48]. 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 espresse da esperti nazionali quanto a una adeguata tutela dei dati raccolti mediante tali strumenti[49]. Per gli stessi motivi, il garante lituano ha sospeso l'analoga applicazione nazionale di controllo dei sintomi[50]. In tale contesto, e al fine di evitare la moltiplicazione di applicazioni diverse eventualmente anche in contrasto con il GDPR e la pertinente giurisprudenza UE, un intervento comune che stabilisse linee guida e salvaguardie appropriate era allora non solo opportuno ma anche necessario.

Ciò è a maggior ragione vero considerato che, come già illustrato, la riapertura dell'area *Schengen* e la piena ripresa della libera circolazione delle persone rende necessaria l'interoperabilità delle singole applicazioni di tracciamento nazionali. Solo la previsione di strumenti il più possibile omogenei dal punto di vista tecnologico e giuridico anche quanto alle cautele poste in essere permetterebbe così di rispondere a tale esigenza del mercato unico. L'interoperabilità delle stesse, auspicata dalla Commissione europea, è stata sollecitata anche da taluni garanti della *privacy*, come quelli italiano e francese[51]. Probabilmente anche a fronte di ciò, il 16 giugno 2020 sono state concordate a livello europeo una serie di specifiche tecniche volte ad assicurare lo scambio sicuro di informazioni tra le applicazioni nazionali di tracciamento[52]. Tuttavia, quantomeno per adesso, tali indicazioni riguardano solo le applicazioni ad

[43] L'applicazione *Immuni* è stata adottata in Italia con art. 6 del decreto legislativo n. 28 del 30 aprile 2020, GU Repub. it. 111 del 30 aprile 2020, poi convertito nella legge n. 70 del 25 giugno 2020 senza apportare alcuna modifica alla detta disposizione. A fronte di ciò, nel presente contributo ci si riferirà allora sempre all'art. 6 d.l. 28.

[44] L'applicazione *StopCovid* francese è fondata sul *décret n° 2020-650* del 29 maggio 2020, il quale è stato approvato dal Parlamento sulla base dell'art. 50-1 Cost. Il testo del decreto è reperibile in www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000041936881&dateTexte=20200702.

[45] Sull'applicazione di tracciamento polacca *ProteGO*, *Report* dell'agenzia europea FRA di aprile 2020 cit., p. 48 e www.natlawreview.com/article/covid-19-poland-launches-official-tracking-app

[46] In Slovacchia è attiva da aprile 2020 l'applicazione di tracciamento *ZostanZdravy*. In merito, *Report* dell'agenzia europea FRA di aprile 2020 cit., p. 48 e https://www.old.korona.gov.sk/en/COVID19-ZostanZdravy.php.

[47] Sull'applicazione *eRouska*, ormai attiva dai primi di aprile 2020, *Report* dell'agenzia europea FRA di aprile 2020 cit., p. 48 e https://english.radio.cz/mobile-app-erouska-now-available-iphone-users-8101241.

[48] In merito, *Report* dell'agenzia europea FRA di aprile 2020 cit., p. 48.

[49] *Ibidem.*

[50] *Report* dell'agenzia FRA di giugno 2020 cit., p. 39.

[51] Garante della *privacy* italiano, *Parere sulla proposta normativa per la previsione di una applicazione volta al tracciamento dei contagi da COVID-19 - 29 aprile 2020 [9328050*], www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9328050, spec. p. 4. Quanto alla Francia, CNIL, *Délibération n° 2020-056 du 25 mai 2020 portant avis sur un projet de décret relatif à l'application mobile StopCovid*, www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000041940832, spec. par. 79.

[52] In merito, v. già riportato alla nt. 27 del presente contributo.

architettura decentrata. Sebbene ciò sia in linea con le direttive della comunicazione UE del 17 aprile 2020 di evitare l'uso di sistemi centralizzati, la previsione delle predette regole tecniche solo per sistemi distribuiti esclude l'interoperabilità di applicazioni che abbiano invece optato per sistemi centralizzati o semi-centralizzati come, ad esempio, quelli italiano e francese[53]. Il fatto tuttavia che la Commissione europea, nella predetta comunicazione, affermi che «la soluzione decentralizzata è *più conforme* al principio della minimizzazione» di cui all'art. 25 GDPR pare escludere la contrarietà del modello centralizzato al GDPR, il quale è così un'opzione possibile seppur non auspicata in quanto meno conforme alla legislazione UE[54].

L'interoperabilità degli strumenti in esame deve inoltre essere assicurata anche migliorando la comunicazione e la cooperazione tra autorità sanitarie nazionali[55], le quali, conformemente all'art. 28 GDPR, devono essere individuate come responsabili del trattamento dei dati sotteso all'uso degli stessi. Tale individuazione, correttamente operata in Italia e in Francia[56], è volta a rafforzare il convincimento che le applicazioni di tracciamento saranno impiegate per finalità solo connesse al contrasto della pandemia, essendo invece escluso un loro uso (e dei dati ivi raccolti) per scopi ulteriori e/o per realizzare una sorveglianza di massa[57].

5. Applicazioni di tracciamento e principio di necessità.

Venendo all'analisi delle singole salvaguardie suggerite nella comunicazione del 17 aprile 2020, la Commissione europea raccomanda innanzitutto agli Stati membri di valutare con serietà l'effettiva necessità (artt. 9 e 23 GDPR) di utilizzare strumenti particolarmente intrusivi della sfera privata degli individui come sono per l'appunto le applicazioni di tracciamento[58]. Sebbene l'esperienza asiatica abbia spesso lasciato la convinzione dell'inevitabile uso della tecnologia per contrastare l'emergenza sanitaria in corso, tali strumenti sono, in realtà, solo uno dei mezzi utili in tali circostanze, il tracciamento manuale svolto con apposite risorse umane restando – in Asia e in Europa – la via maestra per individuare e allertare soggetti entrati in contatto con il virus[59]. A

[53] Su questi aspetti, v. par. 11 del presente contributo.

[54] Così, par. 3.5 (*Limitare la divulgazione di dati/l'accesso ai dati*) della Comunicazione della Commissione europea del 17 aprile 2020 cit. Non si esclude però che un modello di questo tipo possa diventare contrario al GDPR se cumuli al sistema centralizzato altre regole non pienamente rispondenti ai criteri UE.

[55] In tal senso, par. 2 (*Contributo delle app alla lotta al Covid-19*) della Comunicazione della Commissione europea del 17 aprile 2020 cit.

[56] Per l'Italia, art. 6, par. 1, d.l. 28 cit. Quanto alla Francia, art. 1 par. 1, *décret* 2020-650 cit.

[57] Su questi aspetti, v. parr. 7-9 del presente contributo.

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

[59] In tal senso, EDPB, *Linee guida 04/2020* cit., punto 36, nonché espressamente l'art. 6, comma 1, del d.l. 28. Analogamente, la CNIL nella sua *délibération n° 2020-056 du 25 mai 2020* cit. e l'art. 1 del *décret 2020-650* cit. Quanto all'Asia, v., l'esperienza di Singapore come riportata da C. GIROT, *Tracer, non pas traquer: « TraceTogether », l'application mobile de lutte contre le covid-19 de Singapour*, Dalloz-actualité.fr., 16 Aprile 2020.

differenza di quello tecnologico, l'intervento umano permette, infatti, una valutazione dei contatti e dell'epidemia qualitativamente elevata in quanto modulata sulla realtà e le specificità dei singoli collegamenti (contatto al chiuso o all'aperto o in ambienti chiusi con particolari sistemi di circolazione dell'aria; interazione o meno tra soggetti e intensità della stessa; presenza o meno di uno o più strumenti di protezione e tipo di protezioni), nonché fornisce supporto ai soggetti allertati nella delicata fase della gestione della quarantena e dell'isolamento sia prima sia dopo l'esito del test Covid-19 per determinare la positività al virus[60]. Strumenti tecnologici come quelli in esame, pur importanti, sono allora per lo più di appoggio e di completamento al tracciamento manuale, invece sempre necessario, facilitandolo ed accelerandolo.

Anche alla luce dell'appena menzionata complementarietà tra tracciamento manuale e tecnologico, la necessità – ma anche l'efficacia – delle applicazioni in esame è allora da valutarsi in funzione della loro capacità d'interagire con le squadre di tracciamento e, più in generale, di diventare parte integrante della strategia sanitaria nazionale di contrasto alla pandemia. Una volta che il soggetto è avvisato di essere entrato in contatto con il virus tramite la funzione di allerta dei predetti strumenti, esso deve essere immediatamente inserito e assistito dal sistema sanitario, il quale si prende carico di illustrare e guidare il soggetto nell'iter sanitario di accertamento e/o cura della malattia (tempi e modi per effettuare e processare i test Covid-19; comportamenti da tenere anche solo in attesa dell'esito del detto test; modalità di cura di eventuali sintomi, i quali possono peraltro insorgere o mutare in intensità anche dopo aver effettuato il test Covid-19). In mancanza di un tempestivo intervento (ad es., ritardi nei test o assenza di indicazioni sui comportamenti da tenere), la solerte allerta tramite le applicazioni rischia di avere un'utilità limitata (il soggetto allertato ben potrebbe prendere iniziative inadeguate) ed esse non sono allora necessarie in ragione dell'assenza di coordinamento con il sistema sanitario.

La necessità degli strumenti in esame dipende inoltre dalla capacità di eseguire *test* Covid-19. Un utente è avvisato del contatto con il virus solo quando un certo soggetto risulti infetto, condizione che dipende dall'esito di un apposito *test*[61]. La ridotta capacità di eseguire o processare *test* in tempi brevi rallenta – e rende parimenti inefficace – la tempestiva allerta con le moderne tecnologie, non potendo i contatti del soggetto allertato essere individuati e a loro volta avvisati fino a quando il primo non sia stato accertato positivo al virus. Ciò è peraltro ancora più importante considerato che, fino a quando il soggetto allertato non risulti negativo al Covid-19, la libertà di movimento di quest'ultimo fuori dal domicilio (o all'interno se convivente con altri), pur se lasciata all'auto-determinazione dello stesso, è compromessa, potendo essere

[60] In tal senso, 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.

[61] Sulla correlazione tra test Covid-19 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 possono 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.

riacquistata solo a seguito di un apposito *test* con esito negativo. Il fatto di non riuscire a testare o a processare tali *test* in tempi rapidi compromette allora anche diritti fondamentali diversi dalla protezione dei dati, nonché ben potrebbe disincentivare i cittadini dall'installare le applicazioni in esame per evitare, ad esempio, quarantene prolungate in attesa del test Covid-19.

Nonostante l'importanza di questi aspetti preliminari, l'analisi di conformità al GDPR delle legislazioni interne inerenti applicazioni di tracciamento – ove adottate e consultabili – sembra invero essersi concentrata più sui profili di proporzionalità rispetto a quelli di necessità. Quanto a questi ultimi, l'art. 6, comma 1, d.l. 28 si limita, infatti, a stabilire che l'applicazione *Immuni* sarà impiegata tra l'altro per «tutelare la salute attraverso le previste misure di prevenzione n*ell'ambito delle misure di sanità pubblica legate all'emergenza Covid-19*». Inoltre, e pur se l'attività del garante italiano è stata significativa e incisiva nel corso dell'intera procedura di adozione di *Immuni*, tali aspetti, neppure affrontati nei pareri del 29 aprile e del 3 giugno 2020[62], sono solo accennati nel provvedimento del 1° giugno 2020 di autorizzazione dell'applicazione *Immuni*, limitandosi in tale occasione il garante solo a confermare le osservazioni del governo quanto al «particolare contesto emergenziale in cui il trattamento si inserisce e quindi la necessità di adottare misure di contenimento del Covid-19 nel più breve tempo possibile»[63]. Più correttamente, le valutazioni del governo francese quanto all'adozione dell'analoga applicazione *SopCovid* si sono invece fondate sull'analisi di fattori inerenti alla capacità sanitaria alla luce delle indicazioni del Consiglio scientifico Covid-19 e dell'Accademia nazionale di medicina. Il garante francese, ossia la *Commission informatique et liberté* (CNIL), ha poi correttamente dedicato a tali profili l'*incipit* – intitolato proprio «*sur la nécessité…du dispositif*» – delle sue *déliberations* sia del 24 aprile 2020 e sia del 25 maggio 2020[64]. Probabilmente perché pienamente consapevole dell'importanza della valutazione in esame, la CNIL, nella *déliberation* dell'8 maggio 2020, ha inoltre precisato l'esigenza di una periodica rivalutazione della necessità del trattamento dei dati attraverso le applicazioni di tracciamento in funzione dell'evoluzione dell'epidemia[65]. Ciò era invero già stato espresso dal Consiglio di Stato francese nel parere consultivo reso al governo il 4

[62] Per l'Italia, in aggiunta al già citato parere del 29 aprile 2020, v. garante della *privacy*, *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.

[63] Così, il garante della *privacy* italiano nel suo *Provvedimento di autorizzazione al trattamento dei dati personali effettuato attraverso il Sistema di allerta Covid-19 - App Immuni - 1° giugno 2020*, www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9356568, spec. p. 16.

[64] CNIL, Parr. 7-12 *délibération 2020-046 du 24 avril 2020 portant avis sur un projet d'application dénommée StopCovid* (www.cnil.fr/sites/default/files/atoms/files/deliberation_du_24_avril_2020_portant_avis_sur_un_projet_d application_mobile_stopcovid.pdf) e CNIL parr. 3-12 *délibération 2020-056 du 25 mai 2020* cit.

[65] CNIL, *Délibération n° 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, www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000041870579&categorieLien=cid*.

maggio 2020 sul progetto di legge di prolungamento dello stato di emergenza sanitaria in Francia[66].

Dubbi sull'effettiva necessità di applicazioni di questo tipo anche in rapporto alla capacità di risalire alla diffusione del Covid-19 mediante il tracciamento manuale sono stati inoltre manifestati da parte della dottrina nei Paesi Bassi[67]. Dai documenti pubblicati dal governo sull'applicazione olandese ancora in via di elaborazione risulta che quest'ultima non ostacolerà né interferirà con il processo di tracciamento manuale dei servizi di sanità regionali. Considerato che la necessità degli strumenti in esame si fonda proprio sulla capacità d'interagire con le squadre di tracciamento nell'ambito di una politica sanitaria globale, il fatto che il governo olandese escluda invece espressamente ogni interazione tra di essi sembra dimostrare al contrario proprio l'assenza di necessità di un'applicazione di tracciamento. Queste incertezze sono probabilmente tra le ragioni che hanno rallentato l'adozione dello strumento in esame in tale Stato membro, la quale è in effetti ancora allo stadio di mera proposta.

La necessità di applicazioni di tracciamento dovrebbe essere valutata anche in funzione del numero di contagi. Qualora questi ultimi siano ridotti la necessità del tracciamento mediante applicazioni particolarmente invasive dovrebbe, in linea di principio, essere esclusa, potendo essere gestita attraverso il tracciamento manuale, il quale, come già illustrato, resta lo strumento principale per risalire agli individui entrati in contatto con il virus in caso di ogni emergenza sanitaria anche dopo l'avvento delle moderne tecnologie. A fronte di ciò, sorprende allora che la Bulgaria, la Lituania e Cipro, nonostante il basso numero di contagi rilevati, siano stati tra i primi paesi membri a rendere operativa già ad aprile 2020 un'applicazione di tracciamento. Anche considerato che, come si avrà modo di vedere nel prosieguo, essi sono stati tra i pochi Stati membri ad aver scelto l'uso di applicazioni particolarmente invadenti – *location tracing* con GPS e non, come suggerito invece dalla Commissione europea, di *contact tracing* con *Bluetooth*[68] – ciò lascia perplessità quanto all'effettiva esigenza di dotarsi degli strumenti in esame in aggiunta a quelli manuali, nonché, in mancanza di chiare indicazioni nazionali in merito, sull'effettivo svolgimento di analisi circa la necessità.

Indizi sulla (forte troppo) frettolosa corsa da parte dei sistemi nazionali all'uso di applicazioni di tracciamento possono anche trarsi dall'esperienza norvegese. Il 15 giugno 2020 tale Stato SEE ha, infatti, scelto di sospendere l'applicazione *Smittestopp* avviata a maggio 2020 – con cancellazione di tutti i dati raccolti e conservati sul *server* nazionale – in quanto troppo invasiva delle libertà personali (automatica raccolta dei dati inerenti alla localizzazione con GPS e loro conservazione in *server* centrali) in rapporto al (basso) numero dei contagi e alla (elevata) capacità di tracciamento

[66] Par. 7 dell'*avis consultatif* 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.

[67] In tal senso, H. TILANUS, *The Dutch COVID-19 tracing app: A Privacy by Design fiasco?*, in *Privacy Law & Business. International Report*, giugno 2020, p. 12; A. STOLLMEYER, M. SCHAAKE, F. DIGNUM, T*he Dutch tracing app 'soap opera' - lessons for Europe*, https://euobserver.com/opinion/148265.

[68] Su questi aspetti, v. parr. 10 e 11 del presente contributo.

manuale. In effetti, critiche all'applicazione erano già giunte sia dal garante norvegese[69] sia da *Amnesty International* Quest'ultima, nel suo parere di giugno 2020, aveva in effetti qualificato l'applicazione norvegese tra quelle più esposte a un rischio di sorveglianza di massa (insieme a quelle di Bahrein e Kuwait) tra le undici esaminate (oltre ai tre paesi già menzionati, Algeria, Francia, Islanda, Israele, Libano, Qatar, Tunisia e Emirati Arabi)[70].

6. Applicazioni di tracciamento e principio di proporzionalità: legislazioni specifiche e ruolo attivo dei garanti della *privacy*.

Anche al fine di provocare una seria riflessione sull'effettiva necessità di dotarsi di applicazioni di tracciamento, la Commissione europea, nella sua comunicazione del 17 aprile 2020, ha precisato che la decisione sull'adozione di questi strumenti e le loro condizioni di utilizzo che, ai sensi dell'art. 9, par. 2, let. *i*, GDPR, devono essere «appropriate e specifiche per tutelare i diritti e le libertà dell'interessato», sia assunta mediante un apposito strumento normativo di diritto interno (art. 23 GDPR) con il coinvolgimento dei garanti della *privacy* (artt. 35-36 GDPR). E' prima di tutto vista con sfavore la scelta di adattare al caso una previgente legislazione. Ciò è invero comprensibile dato che quest'ultima, adottata per finalità diverse in situazioni non emergenziali, mal si adatterebbe all'uso di strumenti particolarmente invadenti della sfera privata dei cittadini in un contesto invece emergenziale. Anche tenuto conto della particolare sensibilità dei dati personali in discussione, ossia quelli relativi alla salute, solo l'uso di un'apposita normativa permetterebbe in effetti di regolamentare – e all'opinione pubblica di conoscere – il funzionamento (e i limiti di funzionamento) di tali strumenti – il tipo di dati raccolti, i modi e i tempi di conservazione degli stessi, le finalità del trattamento, l'identità del responsabile del trattamento – in tal modo garantendo un livello di trasparenza adeguato agli artt. 12 ss. GDPR.

Nel rispetto di tali indicazioni, l'Italia e la Francia sono stati tra i primi paesi a dotarsi di un'apposita normativa per le applicazioni *Immuni* e *StopCovid* – ossia rispettivamente il d.l. 28 del 30 aprile 2020 poi convertito senza modifiche nella legge 70 del 25 giugno 2020, e il *décret* 2020-650 del 29 maggio 2020. Misure analoghe sono poi in corso di adozione in molti altri Stati membri come, ad esempio, la Spagna[71], il

[69] In tal senso, il garante norvegese https://edpb.europa.eu/news/national-news/2020/temporary-suspension-norwegian-covid-19-contact-tracing-app_de.

[70] *Report Amnesty International* (www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy), giugno 2020.

[71] Sulla Spagna, comunicato governativo ufficiale pubblicato sul sito del Ministero dell'Economia, www.mineco.gob.es/stfls/mineco/prensa/noticias/2020/200623_np_gomera.pdf del 23 giugno 2020.

Belgio[72] e la Finlandia[73]. Ampliando l'orizzonte oltre la UE, scelte più o meno simili sono state effettuate anche in Australia e Singapore. L'app *COVIDSafe* australiana è, infatti, fondata sul *Privacy Amendment Bill* adottato dal parlamento federale a maggio 2020, e l'analoga *TraceTogether* di Singapore opera sulla base del *Privacy Statement*, che si aggiunge al *Personal Data Protection Act* e al *Public Sector Act* inerenti alla raccolta, l'uso e il trasferimento a terzi dei dati rispettivamente nel settore privato e in quello pubblico.[74]

Non sempre tuttavia queste normative possiedono un livello di dettaglio adeguato. In Italia, il d.l. 28, pur se di rango primario, si occupa di disciplinare il funzionamento di *Immuni* (e i suoi limiti) esclusivamente in un capo (il II) contenente un solo articolo (il n. 6). Al fine di favorire la massima trasparenza quanto all'uso di strumenti intrusivi, sarebbe stato opportuno isolarne la regolamentazione in un atto distinto che ne dettagliasse la disciplina in una pluralità di disposizioni e che evitasse di lasciare la definizione di profili essenziali – il tipo di dati raccolti (par. 2, let. *b*), il periodo di trattamento degli stessi (par. 2, let. *e*) o la cessazione della durata del trattamento (par. 6) – a successivi interventi ministeriali. In effetti, la piena comprensione del funzionamento di *Immuni* anche quanto ai profili sopra menzionati deriva dalla lettura dell'art. 6 del d.l. 28 alla luce dei, invece dettagliati, pareri del garante della *privacy*, il quale ha in ogni caso concluso per la complessiva conformità del testo con l'art. 9 GDPR[75].

Più correttamente, il *décret* francese 2020-650 illustra in un unico e autonomo testo – in ogni caso contenete solo sei disposizioni – la disciplina di *StopCovid*. Pur se, anche in questo caso, sarebbe stato auspicabile un maggior dettaglio alla luce delle invece minuziose indicazioni della Commissione europea, il testo francese offre nel complesso 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 alla scelta della Francia d'impiegare il *décret* al posto della legge, la conformità all'art. 9 GDPR pare in ogni caso confermata dal fatto che esso si basi – e sia dunque autorizzato – sull'art. 11 della legge n° 2020-546 del 11 maggio 2020 di prolungamento dello stato di emergenza nazionale, il quale prevede in modo generale il trattamento e la condivisione mediante banche dati dei dati personali relativi alla salute dei soggetti infetti da Covid-19 o di quelli entrati in contatto con il virus[76]. Al fine poi di ottenere

[72] L'*avis* 36/2020 del garante della *privacy* belga del 29 aprile 2020 fa riferimento a due progetti di regi decreti che, quantomeno al momento in cui si scrive, non paiono tuttavia essere stati ancora adottati (www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/AV36-2020.pdf).

[73] Quanto alla Finlandia, v. il comunicato del Ministero della salute finlandese del 12 giugno 2020, https://stm.fi/en/-/koronaviruksen-tartuntaketjujen-katkaisua-tehostavaa-mobiilisovellusta-koskeva-lakiesitys-etenee.

[74] Come rilevato da C. GIROT, *Tracer, non pas traquer* cit., il *Privacy Statement* allinea il *Public Sector Act* (PSGA) al *Personal Data Protection Act* (PDPA), nonché ai principi *Privacy by Design* e *Privacy by Default* di cui all'art. 25 GDPR.

[75] In tal senso, il garante italiano nel suo *Parere sulla proposta normativa 29 aprile 202*0 cit.

[76] www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000041865244&dateTexte=20200715.

il pieno consenso nazionale, il governo ha scelto di usare l'art. 50-1 Cost per sottoporre in ogni caso il predetto decreto a un dibattito e voto (di orientamento) del Parlamento.

Analoghe incertezze quanto all'adeguatezza del testo relativo ad applicazioni di tracciamento sono parimenti da rilevare nelle due proposte di regi decreti belgi di aprile 2020. Come emerge dal già citato parere 36 del garante belga del 29 aprile 2020, infatti, queste proposte era generiche quanto sia alle finalità di utilizzo dei dati raccolti tramite l'applicazione di tracciamento sia all'identità dei soggetti autorizzati ad avere accesso a tali dati. Queste mancanze hanno così indotto il garante a considerare le proposte non pienamente rispondenti al GDPR. Analoghe critiche sono state inoltre mosse alla proposta olandese relativa a una analoga applicazione di tracciamento, la quale, come in effetti quella belga, è ancora allo stadio di mera proposta[77].

E' invece stato più che soddisfacente il coinvolgimento dei garanti della *privacy* nei procedimenti di adozione delle applicazioni di tracciamento. Questi ultimi hanno, infatti, assistito attivamente i governi sia nella fase iniziale di riflessione sull'eventuale adozione degli strumenti in esame mediante il *prior impact assesment* (imposto nel caso di tracciamenti su larga scala dall'art. 35 GDPR) sia lungo tutta la procedura di valutazione degli stessi attraverso linee guida e pareri (artt. 35 e 36 GDPR) in Italia[78], Austria[79], Francia[80], Belgio[81] e Finlandia[82]. Come già illustrato con riferimento al Belgio, è stato spesso l'intervento del garante ad aver indotto i governi nazionali a introdurre opportuni cambiamenti alle proposte normative. Analoghe migliorie sono state poi introdotte in Italia e Francia grazie alle osservazioni dei rispettivi garanti. La Francia, l'Austria e l'Irlanda hanno inoltre richiesto l'attiva partecipazione anche di soggetti ulteriori, ossia rispettivamente la *Commission consultative des droits de l'homme*[83], università e ONG, nonché l'*Attorney General*[84]. Ad eccezione della Bulgaria e dell'Italia, non pare tuttavia che i garanti siano stati chiamati né dai governi né dagli sviluppatori delle applicazioni a una valutazione finale delle applicazioni prima della loro operatività[85], e ciò sebbene tale scelta sarebbe stata auspicabile in base all'art. 35 GDPR.

Quantomeno dall'analisi dei documenti a disposizione, i garanti non paiono invece essere stati sempre coinvolti nell'elaborazione di applicazioni diverse da quelle di tracciamento soprattutto se adottate a livello regionale. A titolo esemplificativo, così sembra essere accaduto per l'applicazione di controllo dei sintomi *AlertLomb* della

[77] Sui Paesi Bassi, H. TILANUS, *The Dutch COVID-19* cit., pp. 12-13.

[78] Con riguardo all'Italia, art. 6, comma 2, d.l. 28 cit. e i già citati pareri del 29 aprile, 1 giugno e 3 giugno 2020.

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

[80] Sul ruolo del CNIL in Francia, v. i già citati pareri del 24 aprile, 8 maggio e 25 maggio 2020.

[81] Il garante belga ha fino ad ora reso (il però determinante) a*vis* 36/2020 cit. del 29 aprile 2020.

[82] Per la Finlandia, *Report* dell'agenzia europea FRA di aprile 2020 cit., p. 52.

[83] CNCDH (Francia), *Avis sur le suivi numérique des personnes* del 28 aprile 2020.

[84] Lo sviluppo di un'applicazione di tracciamento in Irlanda pare in ritardo rispetto alla maggior parte degli altri paesi UE. L'*impact assessment* del garante irlandese è in ogni atteso a luglio 2020. In tal senso, anche con riguardo all'Austria, L. LINKOMIES, *Privacy is the hot issue* cit., p. 11.

[85] *Report* dell'agenzia europea FRA di aprile 2020 cit., p.53.

Regione Lombardia[86] o di quella sul controllo della quarantena in Repubblica ceca[87]. Se così fosse, l'assenza di supervisione del garante nell'elaborazione di applicazioni che, seppur diverse da quelle di tracciamento, implicano il trattamento e la conservazione di dati particolarmente sensibili lascia dubbi sulla conformità delle stesse con gli artt. 35 e 36 GDPR, il che potrebbe tra l'altro condurre in futuro a (invece evitabili) procedure d'infrazione nei confronti dell'Italia per l'errato comportamento delle sue componenti amministrative.

7. *Segue*: le finalità d'uso delle applicazioni nazionali di tracciamento.

La normativa inerente alle applicazioni di tracciamento Covid-19 dovrebbe inoltre essere proporzionata, il che presuppone innanzitutto l'impiego dei dati raccolti tramite questi strumenti solo per conseguire obiettivi correlati al contrasto dell'emergenza sanitaria in corso (artt. 5, let. *b)*, 6, par. 4, e art. 9, par. 2, GDPR). *A contrario*, è dunque esclusa la possibilità che i dati personali ivi raccolti siano usati per scopi ulteriori o diversi come il controllo dell'immigrazione, la sicurezza nazionale o per finalità commerciali, permettendone così l'accesso o il successivo trasferimento a terzi (c.d. trattamenti secondari).

Ora, conformemente alle indicazioni della Commissione, l'art. 6, comma 1, d.l. 28 limita l'uso dell'applicazione *Immuni* alle finalità di interesse generale 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». Considerata l'importanza di quest'aspetto per definire un ambito di applicazione proporzionato degli strumenti in esame, 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. Non è, ad esempio, chiaro in che modo si sostanzi la menzionata «tutela della salute attraverso le previste misure di prevenzione»: ai soggetti allertati sono fornite solo linee direttrici in materia di prevenzione o saranno invece seguiti da appositi servizi sanitari? Le indicazioni fornite sono facoltative o invece obbligatorie? In che modo e tempi essi saranno sottoposti ad apposito test per valutare la loro positività al Covid-19? La mancanza di precisione quanto a questi

[86] In merito, v. il generale (e generico) riferimento del garante della *privacy* italiano di cui al parere del 29 aprile 2020 cit. (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». Sulla impossibilità di valutare la conformità dell'applicazione regionale *AppLomb* alle regole GDPR, F. BOEHM, D. DIMITROVA, F. PICHIERRI, D. 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

[87] In merito, le dichiarazioni del garante (Ivana Jana) del 25 giugno 2020, www.uoou.cz/ochrana-soukromi-v-nbsp-dobe-koronavirove-a-nbsp-projekt-chytra-karantena/d-43029.

aspetti pratici è ancora più evidente se paragonata al par. 2 dell'art. 1 del decreto francese che illustra le quattro funzioni di *StopCovid*, ossia quelle di: 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 fungerà così da guida consigliando gli accorgimenti sanitari da adottare in funzione dei sintomi; d) adattare i parametri d'individuazione dei contatti a rischio attraverso l'uso di dati statistici anonimi.

Ora, pur se il garante italiano ha concluso in ultimo per la conformità del comma 1 dell'art. 6 agli artt. artt. 5, let. *b)*, 6, par. 4, e art. 9, par. 2, GDPR, il non così dissimile livello di genericità dell'art. 3, par. 2, delle proposte di regi decreti belgi – «*1° rechercher et contacter les intéressés…; 2° réaliser des études scientifiques, statistiques et/ou d'appui à la politique; 3° communiquer des données aux services d'inspection de la prévention en matière de santé des régions*» – ha viceversa indotto il garante belga a concludere per la non conformità del testo al GDPR[88].

L'impossibilità di estendere l'uso dei dati raccolti con applicazioni di tracciamento per scopi ulteriori o diversi da quelli indicati in legge è integrata in Italia dall'uso, all'*incipit* del comma 1 dell'art. 6 d.l. 28, dell'espressione «al solo fine di». Le finalità di trattamento dei dati indicate al comma 1 sono dunque tassative e la lista della stesse è così esaustiva. Ciò trova peraltro conferma 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 il comma 1 dell'art. 6 – come il par. 1 dell'art. 1 *décret* francese 2020-650 – abbia individuato nel Ministero della salute il responsabile del trattamento conferma una volta di più la volontà di limitare anche per il futuro il funzionamento delle applicazioni di tracciamento a scopi solo inerenti alla salute pubblica e il contrasto della pandemia.

Quanto ai trattamenti secondari, il garante italiano ne ha escluso la possibilità[89], e ciò sebbene il comma 3 dell'art. 6 del d.l. 28, prevedendo che i dati raccolti con *Immuni* potranno essere impiegati per fini statistici o di ricerca una volta conclusa l'emergenza sanitaria, pare invece autorizzare proprio l'accesso e l'uso degli stessi a terzi. Inoltre, pur se la conformità al GDPR di prescrizioni come quelle in esame è assicurata dall'uso dei dati in forma anonima e aggregata (art. 89 GDPR)[90], al fine di eliminare ogni dubbio su eventuali trattamenti di terzi sarebbe stato opportuno precisare i soggetti che avranno accesso a tali dati (solo le autorità sanitarie elencate al comma 1 art. 6 o anche altri enti terzi?) o prevedere uno specifico consenso. Ciò pare ancor più essenziale considerato che il garante belga, nell'analizzare l'analoga finalità

[88] Parr. 9-13 dell'*avis* 36/2020 cit. del garante belga.
[89] Art. 6, comma 1, d.l. 28 cit. e il parere del garante della *privacy* italiano del 29 aprile 2020 cit.
[90] *Ibiem*, spec. p. 4.

di «*réaliser des études scientifiques, statistiques et/ou d'appui à la politique, après pseudonymisation ou anonymisation*» (art. 3, par. 2, delle proposte di regi decreti) ne ha rilevato la non proporzionalità ai sensi del GDPR proprio per la difficoltà d'individuare i soggetti che avrebbero avuto accesso ai predetti dati per fini statistici o di ricerca[91]. Quanto alla Francia, la lista dettagliata di finalità di cui all'art. 2 del decreto 2020-650 induce a escludere ogni altro trattamento di dati non ivi menzionato. Al riguardo, la CNIL ha inoltre precisato che si deve in ogni caso ritenere esclusa la possibilità di utilizzare i dati raccolti per identificare le aree in cui questi ultimi sono localizzati (geo-localizzazione), monitorare il rispetto delle misure di contenimento, nonché le interazioni sociali delle persone. E' stata invece criticata da parte della dottrina olandese l'eccessiva genericità e scarsa chiarezza della proposta di legislazione dei Paesi Bassi quanto alle finalità e all'uso dei dati personali ivi raccolti[92].

8. Segue: il divieto di una sorveglianza di massa.

La volontà di evitare ogni uso improprio delle applicazioni di tracciamento e allerta – ossia per fini diversi dal contrasto della pandemia – è rinvenibile anche nella richiesta della Commissione europea di inserire in legge l'esplicita esclusione dell'uso dei dati raccolti per fini di sorveglianza di massa[93]. Un riferimento del genere non è tuttavia contenuto né nella legislazione italiana né in quella francese, il che ha indotto la CNIL a precisare, nel suo parere del 25 maggio 2020, che il trattamento dei dati raccolti non dovrebbe mai consentire il monitoraggio delle interazioni sociali delle persone.

Tale previsione non è tuttavia da considerarsi una mera ipotesi di scuola considerato che l'Unione europea è invero già stata confrontata a esperienze di questo genere, o quantomeno a misure nazionali particolarmente invasive della privacy, nel contesto transatlantico (sorveglianza di massa dei servizi di intelligence americani anche rispetto a dati trasferiti dalla UE), con significative conseguenze sul piano giurisprudenziale[94], e in alcuni paesi membri dell'Est Europa. L'Ungheria, pur non disponendo di applicazioni per contrastare l'emergenza sanitaria in corso, a marzo 2020 ha modificato alcune leggi interne che autorizzano ora le autorità di polizia, immigrazione e sanitarie a chiedere (e ottenere) dagli operatori di telecomunicazioni i dati di localizzazione dei cittadini senza il consenso dell'interessato né autorizzazioni della magistratura[95]. Inoltre, invocando pretestuosamente esigenze connesse alla pandemia in corso, l'art. 1 del decreto ungherese 179/2020 del 4 maggio 2020 aveva sospeso l'applicazione delle principali diritti riconosciuti ai cittadini UE dal GDPR, ossia i diritti dell'interessato ad ottenere dal titolare del trattamento (i) la conferma che

[91] Quanto al Belgio, par. 12 de l'*avis* 36/2020 cit.

[92] Sui Paesi Bassi, H. TILANUS, *The Dutch COVID-19* cit., pp. 12-13.

[93] Punto 1 (*Contesto*) della Comunicazione della Commisisone del 17 aprile 2020 cit.

[94] Corte giust. *Schrems* cit. e *Schrems II* cit.

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

sia o meno in corso un trattamento di dati che lo riguardano e, in tal caso, di ottenere l'accesso ai dati trattati (art. 15); (ii) la rettifica (art. 16) o la cancellazione (art. 17) dei dati inesatti che lo riguardano; (iii) il diritto alla limitazione del trattamento (art. 18), (iv) quello di conoscere i terzi a cui siano trasferiti i propri dati dal titolare del trattamento (art. 20); (v) il diritto di opporsi in qualsiasi momento al trattamento dei dati che lo riguardano (art. 21), nonché (vi) di evitare la profilazione (art. 22).

Legislazioni analoghe a quelle ungheresi di marzo 2020 sono peraltro in via di adozione in Polonia, Repubblica ceca, Bulgaria, Romania, Slovacchia, Estonia e Lettonia[96]. In Polonia inoltre vige 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 mancato rispetto delle misure di confinamento[97].

L'adozione di normative 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 (art. 8 della Carta, GDPR e direttiva *e-privacy*, nonché la giurisprudenza UE), ma anche dell'art. 2 TUE[98]. Il fatto peraltro che esse mettano in discussione i valori fondanti l'UE e in particolare quello dello Stato di diritto espone questi ultimi anche alla procedura di cui all'art. 7 TUE, in ogni caso già avviata rispettivamente dal Parlamento europeo e dalla Commissione nei confronti di Ungheria e Polonia per ripetute e pregresse violazioni[99]. Che, anche a fronte del progressivo degradarsi della situazione in tali Stati membri[100], si stia creando un contesto favorevole all'assunzione di una posizione più netta pare emergere dal fatto che le dichiarazioni rese a marzo 2020 dal Presidente della Commissione quanto alla generale necessità di monitorare le misure adottate all'interno dell'UE per fronteggiare la pandemia abbiano trovato il pieno accordo di tredici paesi membri, ossia Belgio, Portogallo, Danimarca, Finlandia,

---

[96] *Report* dell'agenzia europea FRA di aprile 2020 cit., pp. 52-53, nonché D. PETRÁNYI, K. HORVÁTH, M. DOMOKOS, *Hungarian government overwrites the GDPR in its COVID-19 state-of-emergency decree*, .

[97] 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*, www.businessinsider.com/poland-app-coronavirus-patients-mandaotory-selfie-2020-3?IR=C.

[98] Sulle numerose infrazioni dell'Ungheria, Corte giust., 6 novembre 2012, causa C-286/12, *Commissione c. Ungheria*, ECLI:EU:C:2012:687; nonché Corte giust., 20 dicembre 2019, causa C-821/19, ancora pendente. In merito, anche i casi IP/17/5003, IP/17/5004 e IP/1975994. Sull'argomento 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 oarcours 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.

[99] Risoluzione del Parlamento europeo, *GUUE* C 433, 23 dicembre 2019, 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.

[100] Risoluzione del Parlamento europeo del 16 gennaio 2020 sulle audizioni in corso a norma dell'articolo 7, paragrafo 1, TUE, concernenti la Polonia e l'Ungheria (2020/2513(RSP)).

Lussemburgo, Italia, Francia, Germania, Grecia, Irlanda, Paesi Bassi, Spagna, e Svezia.[101] Sebbene si sia ancora lontani dalla maggioranza dei quattro quinti dei membri del Consiglio di cui al par. 1 dell'art. 7 TUE e ancora di più dall'unanimità richiesta in sede di Consiglio europeo dal par. 2 della medesima norma, la forte reazione di ben tredici Stati membri, tra cui i sei fondatori dell'UE, potrebbe portare a nuovi scenari, spingendo, ad esempio, il Consiglio o il Consiglio europeo – fino ad ora inerti per ragioni politiche[102] – ad adottare quantomeno raccomandazioni *ex* art. 7, par. 1, TUE. Ciò pare a maggior ragione vero posto che analoghe preoccupate prese di posizione sono giunte negli ultimi mesi dal Consiglio d'Europa[103] e da altre organizzazioni non governative come *Amnesty International*[104].

Legislazioni interne come quelle sopra descritte potrebbero peraltro essere incompatibili con le stesse Costituzioni nazionali. Ricorsi davanti alle rispettive Corti Costituzionali sono stati in effetti avviati in Bulgaria e Slovacchia e parte della dottrina ritiene essi siano azionabili anche in Ungheria[105]. Ampliando l'orizzonte di indagine, questioni circa la legalità, o perfino la legittimità costituzionale, di misure in base alle quali le autorità governative possono avere accesso a informazioni personali inerenti alla geo-localizzazione e/o l'uso delle carte di credito sono state anche sollevate in Corea del Sud e Israele, ossia in due paesi che rispettivamente ambiscono all'adeguatezza UE e sono già adeguati.

9. *Segue*: L'uso solo temporaneo delle applicazioni di tracciamento.

Lo stretto collegamento richiesto dalla Commissione europea tra applicazioni di tracciamento e lotta al Covid-19 e dunque della necessità degli strumenti in esame è alla base anche dell'indicazione di cui al punto 1 della comunicazione UE del 17 aprile 2020 di circoscrivere temporalmente l'uso di tali tecnologie – e dei dati ivi

---

[101] Per un'analisi dettagliata, P. MORI, *COVID-19, misure emergenziali e Stato di diritto*, https://www.aisdue.eu/web/wp-content/uploads/2020/04/Post-Paola-Mori-Ungheria.pdf.

[102] In merito, L. PECH, *From "Nuclear Option" to Damp Squib? A Critical Assessment of the Four Article 7(1) TEU Hearings to Date*, in *VerfBlog*, 13 novembre 2019.

[103] V. lettera del Segretario generale del Consiglio d'Europa, MARIJA PEJČINOVIĆ BURIĆ, rm.coe.int/orban-pm-hungary-24-03-2020/16809d5f04.

[104] In merito, *Public Statement* di *Amnesty International*, www.amnestyusa.org/wp-content/uploads/2020/03/EUR-27-2046-2020-Amnesty-International-Public-statement-Hungary-COVID19-bill-grants-the-government-extraordinary-power.pdf.

[105] Il ricorso davanti alla Corte Costituzionale bulgara è il n. 4/2020 e, come risulta dal Report dell'Agenzia FRA del 30 giugno 2020 (p. 39) è stato accolta dalla stessa ed è al momento pendente. Per alcune informazioni in inglese, https://sofiaglobe.com/2020/05/14/covid-19-constitutional-court-challenge-against-health-act-amendments-filed/. Il ricorso davanti alla Corte Costituzionale slovacca è stato presentato il 14 aprile 2020 avverso la legge 768/2020. In merito, *Report* dell'Agenzia europea FRA, *Coronavirus pandemic in the EU*, 4 maggio 2020, https://fra.europa.eu/sites/default/files/fra_uploads/sk_report_on_coronavirus_pandemic-_may_2020.pdf. Quanto alla possibilità di avviare analoghi procedimenti in Ungheria, *Report dell'agenzia europea FRA* di aprile 2020 cit., p. 53, nonché B. BAKÓ, B. GYŐRI, P. GALAVITS, *Kémkedhet-e utánunk az állam a koronavírus-járványra hivatkozva?*, https://azonnali.hu/cikk/20200401_kemkedhet-e-utanunk-az-allam-a-koronavirus-jarvanyra-hivatkozva.

raccolti – alla sola emergenza sanitaria in corso, dovendo le applicazioni di tracciamento essere disattivate e i dati personali ivi raccolti cancellati «al più tardi quando la pandemia sia dichiarata sotto controllo» (*sunset clause* di cui all'art. 5 GDPR). Se l'uso di questi strumenti è motivato (o dovrebbe esserlo) dalla sola volontà di contrastare l'emergenza sanitaria, la cessazione della stessa dovrebbe in effetti far venire meno l'utilità delle applicazioni di tracciamento. L'uso dell'espressione «in corso» sottintende allora che l'eventualità di future emergenze non giustificano il mantenimento delle stesse. Il rispetto di questa condizione permette peraltro di ridurre il rischio di un uso improprio dei dati raccolti dalle applicazioni in esame e/o dei casi di sorveglianza di massa, non essendo questi ultimi più accessibili alla fine della pandemia.

La trasposizione nei sistemi nazionali di questa condizione non pare tuttavia sia stata pienamente soddisfacente. Il termine di cessazione del trattamento dei dati – da individuare, per la Commissione europea, in base a un parametro epidemiologiamente oggettivo («quando la pandemia sia dichiarata sotto controllo»), è stato individuato in Italia (art. 6, comma 6, d.l. 28) e Francia (art. 3 *décret 2020-650*) nella conclusione dello stato di emergenza, il quale in Italia è stato decretato con delibera dal Consiglio dei ministri e approvato dal Parlamento, e in Francia è stato promulgato con legge dal Presidente della Repubblica e poi adottato dall'Assemblea nazionale e dal Senato.[106] Essendo la dichiarazione di stato di emergenza (e anche la sua cessazione o la sua proroga) una scelta di politica interna essenzialmente governativa, l'interruzione del trattamento dei dati attraverso le applicazioni di tracciamento varia allora in funzione di un fattore puramente discrezionale difficilmente prevedibile e non, come invece richiesto dalla Commissione, in virtù di un parametro oggettivamente correlato alla pandemia da valutarsi in base, ad esempio, a soglie e valori clinici prestabiliti e prevedibili. La scelta italiana e francese potrebbe allora essere considerata effettivamente proporzionata solo qualora le legislazioni sullo stato di emergenza stabilissero in modo chiaro la cessazione di questa condizione – e dunque anche del trattamento dei dati tramite le predette applicazioni – in funzione di parametri non discrezionali e inequivocabilmente connessi all'emergenza sanitaria, il che tuttavia non pare essere il caso nei due esempi considerati quantomeno a livello legislativo[107]. Né invero tale discrezionalità è limitata in Italia dal fatto che l'art. 6, comma 6, d.l. 28 precisi che il trattamento dei dati attraverso *Immuni* si concluderà «in ogni caso al più tardi il 31 dicembre 2020», ben potendo questa data essere prorogata alla scadenza. La

[106] Sull'Italia, *Dichiarazione dello stato di emergenza in conseguenza del rischio sanitario connesso all'insorgenza di patologie derivanti da agenti virali trasmissibili*, 20A00737, *GU Repub. it., Serie Gen.*, n. 26 del 1 febbraio 2020. Lo Stato di emergenza in Italia dovrebbe essere ulteriormente propagato. Per la Francia, *loi d'urgence n° 2020-290* del 23 marzo 2020 (poi prorogata a maggio), www.legifrance.gouv.fr/affichTexte.do;jsessionid=84A11ADD878E9B78D802D901D1B13966.tplgfr34s_2?cidTexte=LEGITEXT000041746988&dateTexte=20200711.

[107] 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

scelta di ancorare la durata di applicazioni di tracciamento e del trattamento dei dati ivi raccolti allo stato emergenza nazionale potrebbe peraltro indurre i governi a estendere tale condizione eccezionale oltre ciò che sarebbe accettabile per permettere proprio il funzionamento dei predetti strumenti di tracciamento, i quali svolgono la loro funzione più in fasi di contenimento e gestione della pandemia (c.d. fase 2) piuttosto che quando sono introdotte misure di confinamento generalizzato (c.d. fase 1).

Il riferimento alla cessazione dello stato di emergenza, già di per sé incerto, non è peraltro neppure univocamente individuato nei due paesi membri considerati. Mentre in Italia questa condizione coincide esattamente con la durata del trattamento dei dati tramite le applicazioni in esame, concludendosi quest'ultimo quando è previsto cesserà lo stato di emergenza, in Francia quest'ultimo è invece solo il termine iniziale di decorrenza degli ulteriori sei mesi nel corso dei quali è autorizzata la prosecuzione del trattamento dei dati tramite gli strumenti in esame[108]. Ciò peraltro espone la legislazione francese a ulteriori dubbi di compatibilità, andando questa previsione oltre il limite temporale di «al più tardi quando la pandemia sia dichiarata sotto controllo» previsto dalla Commissione europea. Al contempo e a differenza della regola italiana, una previsione come quella francese potrebbe tuttavia permettere di decretare la fine dello stato di emergenza, ossia di una condizione eccezionale per ogni democrazia, senza precludere l'uso delle applicazioni di tracciamento per contenere la diffusione del virus in una fase di generale de-confinamento.

Appare poi in aperto contrasto con l'art. 5 GDPR, anche letto alla luce del principio di proporzionalità, la legislazione polacca relativa all'applicazione di tracciamento dei soggetti in quarantena nella misura in cui stabilisce che tutti i dati personali raccolti – peraltro quelli di localizzazione tramite GPS, nonché le fotografie e i contatti salvati sul dispositivo mobile – saranno conservati per sei anni, ossia un lasso di tempo poco compatibile con una ragionevole durata della pandemia in corso[109].

Anche per tutelare le parti deboli della società che, per scarsa dimestichezza con la tecnologia, abbiano difficoltà a installare, utilizzare e anche disinstallare le applicazioni, la Commissione europea richiede poi che quest'ultima operazione non dipenda dall'iniziativa del singolo utente[110], dovendo essere realizzata dall'esterno nei confronti di tutti gli utenti al più tardi quando la pandemia sia dichiarata sotto controllo. Il fatto che il par. 6 dell'art. 6 del d.l. 28 italiano preveda che «l'utilizzo dell'applicazione e della piattaforma, nonché ogni trattamento di dati personali…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 essere in linea con le indicazioni UE, prevedendo, entro un perentorio *expire time*, la disinstallazione esterna di *Immuni*. Non è invece chiaro se quest'ultima operazione sia prevista in Francia.

[108] Art. 4 della legge francese n° 2020-290 cit. del 23 marzo 2020.

[109] Così, F. BOEHM, D. DIMITROVA, F. PICHIERRI, D. HALLINAN, *Tracking and Tracing Apps* cit.

[110] Punto 3.2 (*Garantire che la persona mantenga il controllo*) della Comunicazione della Commissione europea del 20 aprile 2020 cit.

L'art. 3, par. 2, del *décret* 2020-650 stabilisce che «*la clé d'authentification et l'identifiant aléatoire permanent sont conservés jusqu'à ce que l'utilisateur désinstalle l'application StopCovid*» e sembra lasciare ai singoli utenti il compito di disinstallare l'applicazione. Qualora tuttavia ciò non avvenga, la medesima disposizione prevede la cancellazione «*au plus tard pour la durée mentionnée au premier alinéa*» e dunque al massimo sei mesi dopo la conclusione dello stato di emergenza nazionale. Dalla lettura combinata delle due norme si potrebbe allora desumere che l'utente può in ogni momento disinstallare *StopCovid* e cancellare i dati ivi raccolti. Qualora però quest'ultimo non vi provveda, sarà il sistema, entro il termine indicato, a operare la disinstallazione, la quale avrà così effetti per tutti gli utenti a prescindere dalla loro iniziativa.

La Commissione europea raccomanda inoltre che il codice sorgente delle applicazioni sia reso pubblico e accessibile così da permettere il riesame ad opera di autorità indipendenti[111]. Ciò risponde all'esigenza generale di trasparenza di cui agli artt. 5, par. 1, let. *a*) e 12 ss. GDPR. L'analisi dei vari sistemi nazionali evidenzia come molti di essi – Austria, Cipro, Repubblica ceca, Francia, Italia[112] e Polonia – abbiano già provveduto in tal senso. Come auspicato dalla Commissione europea, in Austria e Repubblica ceca l'esame del codice sorgente ad opera di varie organizzazioni di ricerca ha indotto gli sviluppatori delle applicazioni a introdurre talune modifiche *privacy friendly*[113]. Viceversa, l'incapacità tecnica in Germania di rendere pubblico il codice sorgente ha suscitato aspre critiche da parte degli esperti nazionali.[114] L'adeguamento anche negli altri paesi membri a tale standard UE è allora auspicabile in quanto si tratta di una regola volta a rafforzare la trasparenza di strumenti tecnologici particolarmente intrusivi della sfera privata dei singoli e dunque la fiducia degli utenti anche al fine di massimizzarne l'efficienza, peraltro imposta dall'art. 5 GDPR.

10. Volontarietà dell'installazione e tracciamento dei contatti di prossimità.

La Commissione europea ha anche suggerito una serie di salvaguardie finalizzate a favorire il mantenimento del controllo dei dati personali ad opera dei singoli utenti, a loro volta dirette a rafforzare quella fiducia nelle applicazioni di tracciamento così essenziale per il buon funzionamento delle stesse[115]. A tal fine,

[111] Par. 3.8 (*Garantire la sicurezza dei dat*i) della Comunicazione della Commissione europea del 17 aprile 2020 cit.

[112] In tal senso, espressamente il garante della *privacy* italiano nel parere del 29 aprile 2020 cit., spec. p. 3.

[113] *Report* dell'agenzia FRA di aprile 2020 cit., p. 52.

[114] Così, T. BARKER, *Germany's Angst Is Killing Its Coronavirus Tracing App*, https://foreignpolicy.com/2020/05/08/germany-coronavirus-contract-tracing-pandemic-app/

[115] Par 3.2 (*Garantire che la persona mantenga il controllo*) della Comunicazione della Commissione europea del 17 aprile 2020 cit. In Australia, ad es., a fronte della manifestata volontà di molti attività commerciali e datori di lavoro d'imporne l'uso per il rientro al lavoro o per avere accesso a ristoranti, cinema o eventi pubblici, il governo australiano ha previsto (94H – *Requiring the use of COVIDSafe*) che

l'installazione delle stesse sul proprio dispositivo mobile dovrebbe sempre avvenire su base volontaria e senza conseguenze negative per la persona che decide di non scaricare o utilizzare l'applicazione (il datore di lavoro può imporne al dipendente l'installazione)[116].

L'analisi comparata dei sistemi giuridici mostra come questa condizione sia stata rispettata da tutti gli Stati membri che hanno già adottato o hanno scelto di dotarsi di applicazioni come quelle in esame. Ciò è espressamente previsto all'art. 6, comma 1, del d.l. italiano 28 e all'art. 1, par. 4, del *décret* francese 2020-650. Quest'ultimo precisa anche la gratuità dell'applicazione *StopCovid*. Al fine di evidenziare poi il più possibile la volontarietà delle applicazioni di tracciamento e di rafforzare la fiducia dell'opinione pubblica verso questi strumenti, il par. 4 dell'art. 6 d.l. 28 precisa che il mancato utilizzo di *Immuni* «non comporta alcuna conseguenza pregiudizievole». Fatta eccezione per Stati come Cina, Taiwan e Qatar ove l'installazione di tali applicazioni è obbligatoria, la volontarietà è prevista per lo più anche al di fuori dell'Unione – così in Australia[117], Argentina, Singapore, Corea del Sud e Israele. Tuttavia, come già illustrato, in Israele e Corea del Sud le applicazioni di tracciamento, pur volontarie, sono combinate a un accesso delle autorità governative ai dati di geo-localizzazione o delle carte di credito attraverso una richiesta ai pertinenti servizi nazionali.

E' stato invece rispettato solo da una parte dei paesi membri – ossia Austria, Germania, Danimarca, Francia, Italia, Croazia, Finlandia, Irlanda, Lettonia, Polonia e Portogallo – l'indicazione della Commissione europea d'impiegare la modalità *Bluetooh* a bassa energia (BLE) in luogo di quella GPS. Bulgaria, Cipro e Lituania hanno, infatti, optato per quest'ultima tecnologia e in Slovenia l'applicazione utilizza entrambi i *network*. Ampliando l'orizzonte fuori dall'UE, il *Bluetooh* è usato in Australia[118], Singapore[119] e Svizzera[120]; il GPS è viceversa impiegato in Cina, Corea del Sud, Norvegia, Islanda e Israele[121].

L'uso del *Bluetooth* o del GPS per realizzare applicazioni di tracciamento non è una mera scelta di uno strumento tecnologico tra i tanti possibili sulla base di una loro pretesa equivalenza, essendo invece un fattore indicativo delle intenzioni di un certo sistema di realizzare strumenti conformi al GDPR e proporzionati. L'uso del *Bluetooth* al posto del GPS, come suggerito dalla Commissione, è, infatti, legata non

una persona commette un reato, punibile con il carcere fino a cinque anni e/o con ammende economiche fino a 38 euro, qualora imponga l'installazione dell'applicazione di tracciamento anche solo indirettamente. Così, G. GREENLEAF, K. KEMP, *Australia's 'COVIDSafe' Law for a Voluntary Contact Tracing App*, in *Privacy Laws& Business*, Giugno 2020, p. 1 ss.

[116] Par 3.3 (*Base giuridica per il trattamento*) della Comunicazione della Commissione europea del 17 aprile 2020 cit.

[117] G. GREENLEAF, K. KEMP, *Australia's 'COVIDSafe' Law* cit.

[118] *Ibidem*, pp. 3-4.

[119] In tal senso, C. GIROT, *Tracer, non pas traquer* cit.

[120] Sull'applicazione di tracciamento svizzera, v. i comunicati della *Swiss National Covid-19 Science Task Force*, https://ncs-tf.ch/de/component/edocman/contact-tracing-strategy-26-april-20-en/viewdocument/58?Itemid=0

[121] Per una panoramica sulle applicazioni di tracciamento mondiali, v. i già citati siti web dell'Università VUB di Bruxelles e del *Future of Privacy Forum*.

solo alla maggior accuratezza del primo negli spazi chiusi (centri commerciali, palazzi, autovetture, mezzi di trasporto pubblici),[122] ma anche alla sua maggior conformità ai principi di minimizzazione, *privacy by design* e *privacy by default* di cui all'art. 25 GDPR. La tecnologia *Bluetooth* utilizza i dati generati dallo scambio di segnali tra i dispositivi mobili a una distanza epidemiologicamente significativa (meno di 1 o 2 metri a seconda delle applicazioni) per il periodo epidemiologicamente rilevante (almeno 15 minuti) e permette così di tracciare i contatti tra individui sulla base della sola prossimità dei segnali (*contact tracing*). Diversamente, la tecnologia GPS funziona in base all'esatta localizzazione dell'utilizzatore ed è dunque 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 (*location tracing*). Applicazioni di tracciamento che impieghino la tecnologia GPS vanno allora oltre a quanto necessario per individuare i soggetti entrati in contatto con individui infetti – essendo a tal fine sufficiente la prossimità tra individui – e dunque con i principi di cui all'art. 25 GDPR, fornendo dati sovrabbondanti, ossia quelli di esatta localizzazione degli utenti e del contagio. Il fatto peraltro di disporre di questi ultimi dati potrebbero svelare abitudini e preferenze degli utenti protette da diritti fondamentali diversi a quello in esame. E' quello che è accaduto in Corea del Sud, ove, proprio mediante la tecnologia GPS impiegata[123], è stato possibile, nell'indentificare un diffusore inconsapevole di Covid-19, svelare che il contagio fosse avvenuto in un locale notturno per omossessuali e dunque gli orientamenti del diffusore. Né invero l'uso di applicazioni così invasive sembra escludere il rischio di focolai di contagio. L'esperienza proprio della Corea del Sud e di Israele mostra, infatti, come la diffusione del virus non sia stata limitata dalle predette applicazioni di *location tracing* mediante GPS, essendo tali paesi al momento in cui si scrive confrontati a una recrudescenza dei contagi.

11. Conservazione dei dati personali decentrata o centralizzata?

Sempre al fine di rafforzare la fiducia dei cittadini nelle applicazioni in esame, la Commissione europea, probabilmente prendendo spunto dal modello di Singapore, suggerisce che i dati di prossimità generati dallo scambio di segnali *Bluetooth* tra dispositivi mobili debbano essere conservati – peraltro in forma criptata associando identificativi pseudonimi o anonimi generati arbitrariamente a partire dal numero di

[122] In tal senso, Accesnow.org, *Recommendations on privacy and data protection in the fight against COVID-19*, www.accessnow.org/cms/assets/uploads/2020/03/Access-Now-recommendations-on-Covid-and-data-protection-and-privacy.pdf, p. 9.

[123] La natura particolarmente intrusiva dell'applicazione di tracciamento del governo sudcoreano è stata resa possibile dalla modifica dell'Art. 76-2(2) dell'*Infections Disease Control and Prevention Act* (DCPA) già ai tempi dell'emergenza sanitaria MERS al fine di permettere al Ministro della salute un ampissimo potere quanto alla raccolta – peraltro senza consenso bastando una mera richiesta ai provider di telecomunicazioni – dei dati personali di soggetti sia infetti sia potenzialmente infetti. Tale potere si aggiunge poi a quello previsto all'art. 76-2(1) del medesimo atto che autorizza il ministero della salute a chiedere (e ottenere) da ospedali, farmacie, banche, associazioni di categorie mediche ogni informazione sui propri pazienti. In tal senso, C. GIROT, *Tracer, non pas traquer* cit.

telefono immesso al momento dell'attivazione dell'applicazione – sul dispositivo mobile dell'utilizzatore (c.d. conservazione decentrata o distribuita) e non in *server* nazionali (c.d. conservazione centralizzata)[124]. Pur se entrambe le soluzioni mostrano pregi e difetti e la distinzione tra i due modelli non sia sempre così netta[125], la soluzione decentrata avrebbe più di altre il merito di garantire all'utente il controllo 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.

Nonostante le chiare indicazioni della Commissione europea sull'uso del sistema decentrato e le perplessità sul modello centralizzato rilevate dal Parlamento europeo, dalla gran parte dell'accademia e da talune ONG (tra cui da *Amnesty International*)[126], il primo metodo è stato prescelto solo da Cipro, Estonia, Finlandia, Irlanda, Lettonia, Polonia e Portogallo. Probabilmente a fronte della convinzione iniziale di taluni esperti sull'ambivalenza dei due modelli, molti Stati membri (Austria, Belgio, Bulgaria, Danimarca, Francia, Italia, Lituania, Slovacchia e Repubblica ceca) hanno optato o stanno valutarsi di dotarsi del sistema centralizzato.

La ricostruzione dell'Italia come Stato che ha scelto il sistema centralizzato è stata tuttavia contestata ed è controversa nel nostro paese. Secondo il garante della *privacy*, il fatto che l'art. 6, par. 2, let. e) d.l 28 preveda che «i dati relativi ai contatti stretti *siano conservati anche nei dispositivi mobili degli utenti*» dimostrerebbe in realtà l'utilizzo nel nostro paese di un sistema semi-decentrato. 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 per l'appunto centralmente, essendo invece svolta localmente la verifica degli avvenuti contatti con i positivi a mezzo del confronto tra pseudonimi sugli *smartphone* – si differenzierebbe da modelli totalmente centralizzati, in cui invece entrambi gli adempimenti vengono effettuati centralmente. Una disposizione analoga a quella italiana è peraltro prevista anche in Francia e Austria[127]. Pur nell'incertezza iniziale sul migliore modello da impiegare a cui si è fatto cenno, le chiare indicazioni della

[124] Par. 3.4 (*Minimizzazione dei dati*) della Comunicazione della Commissione europea del 17 aprile 2020 cit.

[125] 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 taluni garanti della *privacy* (quello italiano, ad es., nella *Valutazione d'impatto sulla protezione dei dati personali* del 3 giugno 2020 cit.. pp. 2-3) a ritenere che, in linea di principio, le applicazioni di tracciamento potessero seguire un approccio sia centralizzato sia decentrato.

[126] Risoluzione del Parlamento europeo 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 alla nt. 211.

[127] Quanto alla Francia, art. 2, par. 7, *décret* 2020-650 cit. Quanto all'Austria, L. LINKOMIES, *Privacy is the hot issue* cit., p. 10.

Commissione quanto all'uso di sistemi distribuiti avrebbero tuttavia ben potuto orientare, anche solo in un secondo tempo, gli Stati (e tra questi l'Italia) che avevano inizialmente scelto modelli centralizzati verso quello (pienamente) decentrato più compatibile con il principio di minimizzazione di cui all'art. 25 GDPR, così come peraltro avvenuto in Germania e in Norvegia anche per effetto delle forti critiche interne[128]. Ciò pare ancora più importante considerato che, come illustrato dalla relazione di *Amnesty International* di giugno 2020, il rischio di una sorveglianza di massa (o comunque sproporzionata), sempre evitata, è più elevato in sistemi che abbiano combinato l'uso di metodi centralizzati con la tecnologia GPS. Alla luce di ciò, nell'Unione europea le applicazioni che meglio si prestano a possibili abusi sono allora quelle bulgare, lituane e slovacche. Ampliando l'orizzonte, tale rischio è particolarmente elevato in Cina, Corea del Sud, Bahrein, Kuwait e Qatar[129].

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 le applicazioni di tracciamento avvenga a una duplice condizione, ossia dopo (i) aver accertato l'effettiva positività dell'utilizzatore al Covid-19, e (ii) aver ottenuto da quest'ultimo un apposito consenso (art. 6 GDPR)[130], il quale deve poi essere libero, specifico, esplicito e informato, nonché espresso mediante un'azione positiva inequivocabile[131]. E' 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 risulti infetto al Covid-19, a dare accesso ai dati 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. Ciò è invero comprensibile dato che, come emerge dalla giurisprudenza UE, l'automatico accesso ai dati, senza un'analisi del caso di specie, è incompatibile con un approccio proporzionato[132]. Trattandosi di principi di base per i moderni sistemi di tutela della *privacy*, non sorprende allora che una regola analoga sia in uso anche in paesi extra-UE come l'Australia e Singapore.

---

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

[129] Quanto ai paesi del Golfo, N. STATT, *Gulf states using COVID-19 contact tracing apps as mass surveillance tools, report says*, www.theverge.com/platform/amp/2020/6/16/21293363/covid-19-contact-tracing-bahrain-kuwait-mass-surveillance-tools-privacy-invasion?__twitter_impression=true.

[130] 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.

[131] Par 3.3 (*Base giuridica del trattamento*) della Comunicazione della Commissione europea del 17 aprile 2020 cit.

[132] In aggiunta alla già menzionata Corte giust. *Schrems*, v. ad es. Corte giust. 19 gennaio 1999, causa C-348/96, *Procedimento penale a carico di Donatella Calfa*, ECLI:EU:C:1999:6.

Passando ora all'esame di talune legislazioni, l'art. 1 del *décret* francese 2020-650, conformemente alle indicazioni della Commissione europea, stabilisce che solo una volta ottenuta la diagnosi positiva al Covid-19 gli utenti di *StopCovid* saranno invitati ai passi successivi, ossia la notifica tramite la detta applicazione dei risultati del *test* e la successiva trasmissione al *server* centrale dello storico dei contatti di prossimità raccolti con *Bluetooth*. Tali operazioni non avvengono automaticamente, premurandosi la norma in esame di sottolineare che ognuna di esse è lasciata alla discrezionalità dell'utilizzatore. Pur avendo installato l'applicazione, quest'ultimo è, in altri termini, sempre libero di sottrarsi in qualsiasi momento alla trasmissione alle autorità pubbliche delle informazioni sulla salute e sui contatti di prossimità. La piena liberalità dell'applicazione francese è peraltro ribadita anche in altre disposizioni (artt. 2, 3 e 4). Sebbene la lettura complessiva di quest'ultimo non permetta di comprendere le modalità in cui è prestato l'eventuale consenso all'accesso dei dati, la CNIL ha evidenziato come la volontarietà dell'applicazione si manifesti in tutte le componenti del sistema: installazione, attivazione della comunicazione tramite *Bluetooth*, contatto con un operatore sanitario, notifica della natura positiva della diagnosi e della condivisione dei dati, disinstallazione dell'applicazione[133].

In maniera molto più sintetica – e meno chiara – i parr. 1 e 2 let. *b*) dell'art. 6 d.l. 28 italiano limitano 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. A differenza però del decreto francese, quello italiano non enfatizza la liberalità di *Immuni* in tutte le sue fasi, limitandosi solo ai profili inerenti all'installazione. Come tuttavia ricordato dal garante nel suo parere del 1 giugno 2020, un'applicazione fondata sulla volontarietà degli utenti implica che la volontà si manifesti in tutte le parti del suo funzionamento[134]. Quest'ultimo sembra così un monito al legislatore nazionale a specificare meglio questo profilo invece così essenziale per la compatibilità degli stessi con il GDPR e il loro buon funzionamento.

12. Il tipo di dati raccolti e la conservazione degli stessi in base al principio di minimizzazione.

Quanto alla natura dei dati raccolti, la Commissione europea ricorda che, in base al principio di minimizzazione di cui agli artt. 5, 25 e 89 GDPR, possono essere trattati solo i dati adeguati, pertinenti e limitati a quanto effettivamente necessario. Tali valutazioni – adeguatezza, pertinenza e necessità – devono essere effettuate alla luce delle finalità dell'applicazione – d'informativa, e/o di controllo dei sintomi e/o di tracciamento dei contatti e di allerta – le quali possono anche essere cumulate in un unico strumento (così, ad es., in Austria, Bulgaria, Danimarca, Spagna, Lettonia, Lituania). A titolo esemplificativo, i dati relativi alla salute di una persona non paiono essere rilevanti – e non devono dunque essere raccolti in quanto per l'appunto non

[133] Par. 29 del parere della CNIL del 29 maggio 2020 cit.
[134] Punto 1.1 del parere del garante italiano del 1 giugno 2020 cit.

pertinenti – in applicazioni che si limitino a fornire agli utenti informazioni generali sul Covid-19, mentre lo sono in applicazioni di controllo dei sintomi. Nel caso di applicazioni di tracciamento, i dati utili dovrebbero essere, sulla base di quanto già illustrato, solo quelli di prossimità tra utenti e non quelli di esatta ubicazione degli utilizzatori. Considerato inoltre che i dati trasmessi dall'applicazione devono includere solo identificatori univoci e pseudonimi da rinnovarsi regolarmente 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[135]. 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[136].

Indicazioni analoghe a quelle della Commissione europea si rinvengono anche nel *Privacy Statement* di Singapore inerente all'applicazione *TraceTogether* sviluppata dal Ministero della Salute insieme al *Government Technology Agency*. Esso autorizza, infatti, la raccolta, la conservazione e l'uso solo dei dati di prossimità (e non quelli di geo-localizzazione), nonché esclude l'accesso a ogni ulteriore dato personale come il nome e l'indirizzo dell'utente o la lista di contatti registrata sul dispositivo mobile di quest'ultimo. In realtà, e seppur al solo fine di migliorare il funzionamento dell'applicazione *TraceTogether*, è possibile risalire ad altre informazioni personali (marca, modello e versione IOS dell'apparecchio) e/o dell'applicazione (versione, paese, lingua e durata dell'installazione).

Nonostante le indicazioni di dettaglio fornite dalla Commissione europea quanto al tipo di dati da raccogliere, un'analisi comparata dei sistemi nazionali mostra come spesso le legislazioni interne alla base di applicazioni di tracciamento manchino di dettagli quanto a tale aspetto invece così essenziale. In Italia, l'art. 6, par. 2, let. *b*) d.l 28 si limita a stabilire che i dati raccolti dall'applicazione «siano esclusivamente quelli necessari ad avvisare gli utenti...di rientrare tra i contatti stretti di altri utenti accertati positivi al COVID-19» e la let. *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. E' in effetti solo alla luce delle indicazioni del garante di cui al suo parere del 1 giugno 2020 che emerge la generale conformità del sistema di conservazioni dei dati italiano al principio di minimizzazione 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

[135] Par. 3.2 delle linee guida del EDPB 04/2020 del 21 aprile 2020 cit.

[136] Par. 3.5 (*Limitare la divulgazione di dati/l'accesso ai dati*) della Comunicazione della Commissione europea del 17 aprile 2020 cit.

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*).

Più correttamente, l'art. 2 del *décret* francese 2020-650 contiene, già a livello legislativo, la lista, peraltro esaustiva, dei dati che *StopCovid* raccoglie, conserva e usa per perseguire le finalità menzionate all'art. 1 del predetto decreto. Le osservazioni della CNIL contenute nel parere del 25 maggio 2020 hanno indotto peraltro le autorità francesi ad integrare la lista di cui all'art. 2, inserendo, per ragioni di trasparenza, una serie di dati che, pur se effettivamente raccolti e conservati dall'applicazione, non vi figuravano, ossia «*la collecte des périodes d'exposition des utilisateurs à des personnes contaminées, les codes pays et la collecte des dates de dernière interrogation du serveur*». In Belgio, la genericità delle informazioni relative ai dati raccolti, conservati e usati di cui all'art. 2 dei progetti di regi decreti è stata poi criticata dal garante belga nel suo parere n. 36/2020. Analoghe critiche sono state inoltre mosse alle legislazioni alla base delle applicazioni australiana[137] e olandese[138].

Un medesimo livello di genericità delle legislazioni nazionali è peraltro da rilevarsi quanto alla durata della conservazione dei dati personali raccolti tramite le applicazioni di tracciamento, la quale, in virtù dell'art. 5 let. *e)* GDPR, non può essere più lunga di quanto necessario ed è da determinarsi in base alle diverse funzionalità dell'applicazione.[139] Nonostante la Commissione europea, nella sua comunicazione del 17 aprile 2020, avesse indicato il termine massimo di un mese (21 giorni di incubazione della malattia e margine di azione) per le applicazioni di tracciamento[140] l'art. 6, comma 2, let. e) del d.l. 28 italiano si limita, in modo generico, ad affermare che «vi dati...siano conservati…per il periodo strettamente necessario al trattamento, *la cui durata è stabilita dal Ministero della salute*». Solo la lettura della valutazione di impatto del garante 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, quanto ad applicazioni di tracciamento, esso abbia anche già individuato un limite temporale di cancellazione, peraltro ridotto rispetto a quello indicato dalla Commissione, ossia 14 giorni quanto ai dati memorizzati sia sui dispositivi mobili degli utenti sia nel *backend* di *Immuni*. Non è chiaro tuttavia quale sia il momento iniziale di decorrenza del predetto periodo. 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 sul dispositivo mobile di un certo

[137] In tal senso, G. GREENLEAF, K. KEMP, '*Australia's COVIDSafe Experiment, Phase III: Legislation for Trust in Contact Tracing*', 15 maggio 2020, *University of New South Wales Law Research Series*. ssrn.com/abstract=3601730.

[138] Così, H. TILANUS, *The Dutch COVID-19* cit., pp. 12-13.

[139] Par. 3.5 (*Definire limiti rigorosi per la conservazione dei dati*) della Comunicazione della Commissione europea del 17 aprile 2020 cit.

[140] Punto 3.7 (*Definire limiti rigorosi per la conservazione dei dati*) della Comunicazione della Commissione europea del 17 aprile 2020 cit.

soggetto siano conservati per 15 giorni dalla loro registrazione attraverso *StopCovid*. Il medesimo termine è poi previsto sempre all'art. 3 anche per i dati della cronologia di prossimità dei contatti a rischio di contaminazione condivisi sul *server* centrale. Il termine di conservazione è invece indicato in 30 giorni in Austria[141] e in 21 giorni a Singapore e in Australia[142].

Il fatto che la legislazione sia italiana sia francese abbiano previsto periodi di tempi 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 UE del 17 aprile 2020, un lasso di tempo di conservazione più breve di un mese qualora la persona sottoposta a tampone risultasse negativa. Considerato che la funzionalità delle applicazioni di tracciamento è legata alla positività Covid-19, l'indicazione di tempi ridotti in caso di negatività sarebbe invero stata opportuna anche a fronte di tempi di conservazione ridotti rispetto a quelli previsti dalla Commissione europea.

13. Conclusioni.

Una serie di considerazioni possono trarsi dall'analisi compara svolta nei paragrafi precedenti. Innanzitutto, che, confrontati alla difficile prova di rivedere il bilanciamento tra il diritto alla protezione dei dati e quello alla salute per far fronte alla pandemia Covid-19, molti Stati membri hanno reagito in modo responsabile, mettendo la tecnologia a servizio della collettività senza per questo pregiudicare, quantomeno in modo eccessivo o irrimediabile, i diritti fondamentali nazionali e UE. Tuttavia, soprattutto a fronte degli evidenziati vantaggi del tracciamento manuale rispetto a quello tecnologico, sarebbe stata auspicabile un'analisi più approfondita ad opera dei governi nazionali (e talvolta di alcuni garanti) sull'effettiva necessità di dotarsi di applicazioni di tracciamento, per natura particolarmente invasive della sfera privata dei singoli, per risalire ai soggetti entrati in contatto con il virus. 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 (attesa degli esiti del test, quarantena e isolamento, gestione delle relazioni al domicilio ad es. con famigliari magari non positivi al Covid-19) – sarebbe forse potuto essere la migliore soluzione, permettendo in ogni caso il tracciamento dei contatti e la sicurezza pubblica senza pregiudicare eccessivamente il diritto di cui all'art. 8 della Carta fondamentali.

[141] Così, F. BOEHM, D. DIMITROVA, F. PICHIERRI, D. HALLINAN, *Tracking and Tracing Apps* cit., p. 8.

[142] Quanto a Singapore, C. GIROT, *Tracer, non pas traquer* cit. Per l'Australia, G. GREENLEAF, K. KEMP, *Australia's 'COVIDSafe' Law* cit., p. 3.

Qualora poi un certo Stato abbia scelto di dotarsi di applicazioni di tracciamento, le legislazioni istitutive di queste ultime si sono spesso dimostrate carenti di regole di dettaglio quanto al funzionamento (e ai limiti di funzionamento) degli strumenti in esame. E ciò sebbene tale risultato di trasparenza sarebbe stato 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 (per definizione) generale del GDPR. Né invero i governi nazionali sembrano aver sfruttato appieno le conoscenze e i suggerimenti dei garanti della *privacy*. Sebbene essi abbiano partecipato attivamente al procedimento di elaborazione delle legislazioni interne alla base di applicazioni di tracciamento, le spesso numerose e dettagliate linee guida di questi ultimi non hanno in effetti sempre condotto a normative parimenti dettagliate. Fatta eccezione per quest'ultimo profilo in ogni caso per lo più imputabile ai governi nazionali, l'analisi svolta evidenzia il contributo essenziale reso dai garanti nel contesto in esame. Come auspicato dal GDPR, essi si sono, infatti, dimostrati attori principali di un procedimento normativo (almeno potenzialmente) virtuoso e dunque soggetti indispensabili per le moderne democrazie nell'era digitale. Il loro intervento non è peraltro consistito in un mero controllo – per così dire a valle – della conformità al GDPR della legislazione interna, ma si è sostanziato in un contributo attivo all'elaborazione dello stesso strumento normativo, ossia in un intervento per così dire a monte dello stesso. 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 a breve l'effettiva interoperabilità delle applicazioni nazionali di tracciamento, così da rispondere pienamente alle esigenze del mercato unico.

La valutazione dei comportamenti dei paesi membri nel corso della pandemia non ha però mostrato solo esempi virtuosi. Altri Stati membri non sono stati, infatti, all'altezza della sfida posta dal Covid-19, dando la concreta impressione di utilizzare l'emergenza sanitaria per finalità, puramente interne, di sorveglianza (anche di massa) dei propri cittadini, richiamando così modelli del passato. Ciò invero non sorprende considerato che questi stessi paesi membri si sono già più volte dimostrati – nel passato, nel presente e probabilmente anche in futuro – non sempre adeguati ai valori UE di cui all'art. 2 TUE, ossia a una condizione essenziale anche solo per diventare un paese membro dell'Unione (art. 49 TUE).

Pur con i limiti evidenziati, le applicazioni di tracciamento in uso nella maggior parte dei paesi membri hanno tuttavia dimostrato di avere robuste *privacy policies* di cui al GDPR, soprattutto se paragonate a quelli di Stati extra-UE come Corea del Sud, Israele, India, Messico, Bolivia, Kenya e Sud-Africa[143]. Sorprende peraltro che paesi adeguati ai sensi dell'artt. 45 GDPR (Israele) o che aspirano a tale adeguatezza (Corea

[143] In tal senso, *International Digital Accountability Council* (IDAC), *Privacy in the Age of COVID:An IDAC Investigation of COVID-19 Apps*, 5 giugno 2020, https://digitalwatchdog.org/wp-content/uploads/2020/06/IDAC-COVID19-Mobile-Apps-Investigation.pdf., spec. p. 6.

del Sud) abbiano adottato legislazioni e applicazioni di tracciamento particolarmente invadenti in contrasto con moderni modelli di tutela dei diritti fondamentali, il che, come illustrato, potrebbe pregiudicare in futuro la loro adeguatezza agli *standard* europei. Ciò pare a maggior ragione vero considerata la particolare severità della Corte di giustizia dell'Unione europea nel valutare la conformità all'art. 8 della Carta dei diritti fondamentali di decisioni di adeguatezza adottate dalla Commissione europea con Stati terzi (così la recente pronuncia *Schrems II* del 16 luglio 2020 con riguardo agli USA). Viceversa, è da rilevare come altri sistemi extra-UE (Singapore, Svizzera, Australia) abbiano optato per modelli legislativi e tecnologici simili a quelli europei, in tal modo confermando una volta di più[144] come il GDPR rappresenti sempre più un punto di riferimento a livello internazionale.

[144] In tal senso, SERENA CRESPI, *Il trasferimento dei dati personali UE in Stati terzi* cit.