INSIGHT

LE CONDIZIONI RICAVABILI DAL REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PER LE APPLICAZIONI NAZIONALI DI TRACCIAMENTO DEI CONTATTI: ALCUNE CONSIDERAZIONI

GABRIELE RUGANI*

ABSTRACT: In order to manage the COVID-19 pandemic, several EU Member States have decided to use contact tracing apps, which can display different characteristics: some of them rely on Bluetooth technology, while others on GPS location; some of them adopt a decentralised approach in data collection, while others a centralised approach. The present *Insight* focuses on the conditions that such apps must follow in order to be respectful of the General Data Protection Regulation (GDPR). First of all, it is necessary to choose a suitable legal basis for the processing, remembering that when sensitive data (such as health data) are collected the range of possibilities is even narrower. Depending on such choice, the processing is subject to different limits. Secondly, there are many principles which must be followed in any case, such as purpose limitation, data minimisation and storage limitation. Finally, the data subject must be put in a position to exercise his rights, and the data controller must fulfil obligations such as carrying out an impact assessment and adopting adequate security measures. Taking into consideration such conditions, it seems clear that according to the GDPR some contact tracing apps are more preferable than others, depending on their characteristics. In conclusion, it is possible to state that the GDPR balances public health and data protection by suggesting a graduality principle: the less privacy-invasive solution must be chosen, and it can be incremented only if the purposes cannot be sufficiently achieved. It is the only way to build trust in the users and therefore guarantee the effectiveness of the measures.

KEYWORDS: COVID-19 and the EU – general data protection regulation (GDPR) – data protection – contact tracing apps – data minimisation – health data.

I. INTRODUZIONE

Tra le innumerevoli sfide che hanno interessato il quadro giuridico dell'Unione europea in ragione della pandemia da COVID-19, una delle più significative è senza dubbio quella che riguarda la disciplina in materia di protezione dei dati personali. In particolare, ci si

* Dottorando di ricerca in Scienze giuridiche, Università di Pisa, gabriele.rugani@phd.unipi.it.

ISSN 2499-8249
doi: 10.15166/2499-8249/385

interroga su quali siano le condizioni ricavabili dal celebre Regolamento (UE) 2016/679,[1] meglio noto come GDPR ("*General Data Protection Regulation*"), per le applicazioni nazionali di tracciamento dei contatti, o "*contact tracing apps*": queste ultime potrebbero rappresentare un valore aggiunto nell'ottica del contenimento dei contagi, poiché aiuterebbero a individuare chi, avendo precedentemente interagito con un malato di COVID, corre un rischio significativo di essere stato contagiato.

Tra gli Stati dell'UE che hanno deciso di avvalersi di simili applicazioni è possibile citare, innanzitutto, l'Italia: dal 15 giugno 2020 è stata infatti attivata su tutto il territorio nazionale "Immuni",[2] app su base volontaria che si avvale della tecnologia *Bluetooth Low Energy*.[3] Semplificandone il funzionamento, ad ogni dispositivo viene associato un codice casuale e, quando un utente entra in contatto con un altro utente, i dispositivi si scambiano i rispettivi codici. Là dove poi un utente risulti positivo al COVID-19, quest'ultimo può mettere a disposizione le informazioni circa i suoi recenti incontri. Infine, tali informazioni vengono utilizzate per avvertire chi ha avuto un contatto a rischio con la persona infetta, indicandogli altresì la procedura da seguire.[4] Per quanto invece riguarda la modalità di conservazione dei dati, l'app "Immuni" fa ricorso a un approccio c.d. "decentralizzato":[5] esso comporta che i dati relativi alle interazioni vengano archiviati solo sui dispositivi degli utenti,[6] i quali poi si connettono al server solo per controllare se tra gli identificativi delle persone risultate positive vi sia qualcuno dei codici memorizzati.[7]

Sempre a titolo esemplificativo, anche la Germania ha optato per un'app su base volontaria, che utilizza la tecnologia *Bluetooth Low Energy* e che, nella conservazione dei dati, segue un approccio decentralizzato:[8] si tratta dell'applicazione "Corona-Warn-App".[9]

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

[2] App immuni: www.immuni.italia.it.

[3] Governo italiano, Presidenza del Consiglio dei Ministri, *Al via "Immuni", l'app per il contact tracing*, 3 giugno 2020, www.governo.it.

[4] S. Rossello, P. Dewitte, *Anonymization by decentralization? The case of COVID-19 contact tracing apps*, in *European Law Blog*, 25 maggio 2020, europeanlawblog.eu.

[5] Garante per la protezione dei dati personali, Provvedimento di autorizzazione al trattamento dei dati personali effettuato attraverso il Sistema di allerta Covid-19 – App Immuni, 1 giugno 2020, www.garanteprivacy.it.

[6] F. Boehm, D. Dimitrova, F. Picchierri, 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*, in *FIZ Karlsruhe*, Aprile 2020, www.fiz-karlsruhe.de, p. 13.

[7] E. Cirone, *L'app italiana di contact tracing alla prova del GDPR: dall'habeas data al ratchet il passo è breve?*, in *SIDIBlog*, 13 maggio 2020, www.sidiblog.org.

[8] R. Barcelo, S. Belovicova, S. Faber, P. Věžníková, M. Langhofer, M. Gad-Nowak, I. Fernández, A. Ibraimova, M. Kirk, *An Overview of the EU and National Guidance and Approaches to Contact Tracing Apps With a Focus on Data Protection Issues*, in squirepattonboggs.com, Giugno 2020, www.squirepattonboggs.com, p. 9.

[9] Corona-warn app, *Corona-Warn-App Open Source Project*, www.coronawarn.app.

Prendendo poi in considerazione altri Stati, si può notare come il modello appena descritto per Italia e Germania sia il più frequente[10] (si può menzionare in questo senso anche l'app "Stopp Corona" austriaca);[11] vi sono però anche altri paradigmi, come quello adottato dalla Francia: l'app "Stop Covid",[12] pur essendo a base volontaria e avvalendosi a sua volta del *Bluetooth*, è contraddistinta da un approccio centralizzato, che per l'appunto prevede la conservazione dei dati su un server centrale;[13] i dispositivi, infatti, inviano periodicamente a tale server la lista degli identificativi con cui sono entrati in contatto.[14]

Deve inoltre essere menzionato il fatto che alcune applicazioni non utilizzano la tecnologia *Bluetooth*, ma la localizzazione GPS (*Global Positioning System*): è il caso dell'app slovacca "Zostaň zdravý",[15] dell'app cipriota "CovTracer",[16] nonché dell'app bulgara "ViruSafe".[17]

L'obiettivo del presente contributo è dunque quello di evidenziare quali sono le condizioni che un'applicazione nazionale deve rispettare ai sensi del GDPR al fine di proteggere al meglio i dati personali degli utenti. Verrà altresì effettuata una comparazione tra le caratteristiche delle app concretamente sviluppate dagli Stati dell'Unione e poc'anzi menzionate, in modo da mettere in luce quali di esse siano maggiormente conformi alla disciplina UE in materia di *data protection*.

II. La compatibilità generale delle applicazioni di tracciamento con il GDPR

In primis, è necessario precisare che il quadro normativo esistente non osta alla predisposizione di simili applicazioni. Ciò è confermato sia dal dato testuale del GDPR (come si vedrà), sia dal Comitato europeo per la protezione dei dati ("*European Data Protection Board*" o EDPB): quest'ultimo è un organismo dell'Unione, disciplinato dal Capo VII Sezione 3 del Regolamento[18] e composto dalle figure di vertice delle autorità di controllo degli Stati membri e dal Garante europeo della protezione dei dati.[19] Il Comitato, infatti, a partire dal mese di marzo del 2020 si è espresso in più di un'occasione sulle proble-

[10] Per un confronto tra *contact tracing apps*, si veda A. Tomaschek, *Comparing Contact Tracing Apps for Coronavirus around the World*, in *proprivacy.com*, 18 giugno 2020, proprivacy.com; si veda anche Vrije Universiteit Brussel – Law, Science, Technology & Society Research Group, *Contact Tracing Apps*, lsts.research.vub.be.

[11] App Stopp corona: www.stopp-corona.at.

[12] App Stop covid: www.gouvernement.fr.

[13] R. Barcelo, S. Belovicova, S. Faber, P. Věžníková, M. Langhofer, M. Gad-Nowak, I. Fernández, A. Ibraimova, M. Kirk, *An Overview of the EU and National Guidance*, cit., p. 8.

[14] E. Cirone, *L'app italiana di contact tracing*, cit.

[15] App Zostaň zdravý, www.zostanzdravy.sk.

[16] App CovTracer, covid-19.rise.org.

[17] App ViruSafe, virusafe.info.

[18] Art. 68-76 del Regolamento 2016/679, cit.

[19] *Ibid*., art. 68, par. 3.

matiche relative al trattamento dei dati personali nell'attuale contesto di emergenza e ha dunque contribuito a mettere alcuni punti fermi.

Già in data 19 marzo 2020, con uno "*Statement on the processing of personal data in the context of the COVID-19 outbreak*",[20] il *Board* ha precisato che le norme in materia di protezione dei dati come il GDPR non ostacolano l'adozione di misure per il contrasto della pandemia di coronavirus[21]. Ancora, nelle "*Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*",[22] adottate dal Comitato il 21 aprile, si sottolinea che il quadro normativo in esame è stato concepito per essere flessibile e, in quanto tale, è in grado di conseguire una risposta efficace per limitare la pandemia e proteggere i diritti umani e le libertà fondamentali.[23] Inoltre, in risposta ad una lettera degli Europarlamentari Lucia Ďuriš Nicholsonová e Eugen Jurzyca del 23 marzo,[24] il 24 aprile l'EDPB ha precisato con ancora più chiarezza che "*there is no need to lift GDPR provisions but just to observe them*", dal momento che la disciplina UE in materia di *data protection* prende già in considerazione le operazioni di trattamento necessarie a contribuire alla lotta contro un'epidemia.[25] Quest'ultima affermazione, in particolare, trova esplicito riscontro nel dato letterale: la prova che il legislatore dell'Unione aveva già previsto una simile eventualità all'interno del Regolamento è infatti rappresentata dal considerando 46 (su cui si tornerà anche in seguito), in cui viene prospettata come configurabile l'ipotesi di un trattamento "necessario [...] per tenere sotto controllo l'evoluzione di epidemie e la loro diffusione".

III. L'individuazione della "base giuridica" del trattamento e i limiti derivanti dalla stessa

È ora necessario capire a che condizioni possano essere adottate misure per il contrasto della pandemia come il tracciamento dei contatti. In primo luogo, occorre trovare al trattamento dei dati personali una giustificazione, che nello specifico prende il nome di "base giuridica"[26]. L'art. 5, par. 1, lett. a), del Regolamento prevede infatti che i dati personali debbano essere "trattati in modo lecito" (c.d. principio di "liceità"); e, secondo l'art. 6, il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle basi

[20] European Data Protection Board, Statement of 19 March 2020 on the processing of personal data in the context of the COVID-19 outbreak, edpb.europa.eu.

[21] *Ibid.*, p. 1.

[22] European Data Protection Board, Guidelines 04/2020 of 21 April 2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, edpb.europa.eu.

[23] *Ibid*., p. 3.

[24] *Koronavírus: Nicholsonová a Jurzyca žiadajú EÚ, aby zmenila prístup k GDPR*, in www.aktuality.sk.

[25] European Data Protection Board, Response of 24 April 2020 to Mrs Ďuriš Nicholsonová and Mr Jurzyca's letter on common guidance in the fight against the COVID-19 pandemics, edpb.europa.eu, p. 1.

[26] G. Comandé, G. Malgieri (a cura di), *Manuale per il trattamento dei dati personali – Le opportunità e le sfide del nuovo Regolamento europeo sulla privacy*, Milano: Il Sole 24 Ore, 2018, p. 33 *et seq*.

giuridiche contenute nel par. 1 (ma in molte situazioni, come quella in esame, vi sono più alternative possibili tra cui optare).

La base giuridica più nota è rappresentata dal consenso della persona interessata,[27] che può essere posto a fondamento di un trattamento anche nel caso di specie. Ma in tale ipotesi devono essere soddisfatti tutti i rigorosi requisiti previsti:[28] in particolare, il consenso deve essere libero, specifico, informato, inequivocabile e dato mediante dichiarazione o azione positiva.[29] Tale base giuridica viene indicata, ad esempio, in relazione all'app tedesca "Corona-Warn-App"[30] e all'app austriaca "Stopp Corona".[31]

Altre due basi giuridiche a cui si può far ricorso nell'ipotesi in questione sono poi la necessità del trattamento "per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica"[32] e la necessità del trattamento "per l'esecuzione di un compito di interesse pubblico".[33] Ad indicare la loro validità nel caso in esame è il già menzionato considerando 46, che cita i trattamenti necessari "per tenere sotto controllo l'evoluzione di epidemie e la loro diffusione" come esempio di caso in cui la giustificazione può essere rappresentata tanto dagli interessi vitali dell'interessato, quanto da rilevanti motivi di interesse pubblico. I primi vengono menzionati, a titolo esemplificativo, in riferimento all'app slovacca "Zostaň zdravý" (insieme al consenso).[34] Ma i secondi parrebbero rappresentare, in assoluto, la base giuridica più pertinente a costituire il fondamento di liceità per un'app di tracciamento dei contatti: in tal senso si è espresso infatti l'EDPB;[35] inoltre, i motivi di interesse pubblico vengono indicati come giustificazione del trattamento in relazione a numerose app, come l'italiana "Immuni"[36] e la francese "Stop Covid".[37]

Sempre in tema di base giuridica, occorre però fare ulteriori precisazioni. L'art. 9 del Regolamento, infatti, prevede delle condizioni ancora più stringenti per il trattamento di "categorie particolari di dati": tale trattamento in linea di principio è addirittura vietato,[38] a meno che non si verifichi uno dei casi elencati nel par. 2. Una simile disciplina è motivata dal fatto che le categorie di dati personali in questione, per loro natura, sono particolarmente sensibili, "dal momento che il contesto del loro trattamento potrebbe

[27] Art. 6, par. 1, lett. a), del Regolamento 2016/679, cit.
[28] Guidelines 04/2020 adopted on 21 April 2020, cit., p. 8.
[29] Art. 4, n. 11, del Regolamento 2016/679, cit.
[30] "Corona-Warn-App", *Privacy Notice*, www.coronawarn.app, par. 3.
[31] "Stopp Corona" App, *Data Protection Information*, par. 4.2.
[32] Art. 6, par. 1, lett. d), del Regolamento 2016/679, cit.
[33] *Ibid*., art. 6, par. 1, lett. e).
[34] Aplikácia "Zostaň zdravý", *Informácie GDPR*, www.zostanzdravy.sk, par. 4.
[35] Guidelines 04/2020 adopted on 21 April 2020, cit., p. 7.
[36] App "Immuni", Informativa Privacy, www.immuni.italia.it, par. 3.
[37] Application "StopCovid France", *Données personnelles*, bonjour.stopcovid.gouv.fr.
[38] Art. 9, par. 1, del Regolamento 2016/679, cit.

creare rischi significativi per i diritti e le libertà fondamentali";[39] il maggior rischio, in particolare, è quello di una discriminazione.[40]

Tra i dati sensibili dell'art. 9, par. 1, sono menzionati anche i "dati relativi alla salute", ovvero "dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute".[41] Orbene, non vi è dubbio che il ricorso a un'app per fronteggiare la pandemia da COVID-19 possa portare anche alla raccolta di dati relativi alla salute: ad esempio, lo *status* di persona infetta.[42] Da ricordare che il Gruppo di lavoro articolo 29 (poi sostituito dall'EDPB con l'entrata in vigore del Regolamento 2016/679), già il 5 febbraio 2015 si era espresso proprio sugli "*health data in apps and devices*",[43] precisando che i dati trattati a mezzo di applicazioni sono da considerare sanitari se l'applicazione ha finalità *lato sensu* diagnostiche o comunque tratta dati che permettono facilmente di dedurre informazioni sullo stato di salute. Non c'è dubbio che i dati riguardanti, come appena detto, la positività al virus di un individuo rientrino in questa categoria.

Occorre dunque giustificare il trattamento di tali categorie di dati ai sensi del par. 2 dell'art. 9. La prima base giuridica a cui far riferimento è quella dell'art. 9, par. 2, lett. i).[44] Tale disposizione, infatti, riguarda l'ipotesi della necessità del trattamento per motivi di interesse pubblico nel settore della sanità pubblica, "quali la protezione da gravi minacce per la salute a carattere transfrontaliero"; il trattamento in questione, tuttavia, deve avvenire sulla base del diritto dell'UE o degli Stati membri,[45] che deve altresì prevedere "misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale". La disposizione in esame viene invocata a fondamento del trattamento dei dati sensibili nel caso, ad esempio, dell'app "Immuni".[46]

Ci sono comunque altre possibili basi giuridiche[47]. Tra di esse, la necessità del trattamento per finalità di assistenza sanitaria,[48] la necessità del trattamento a fini di ricerca scientifica o a fini statistici,[49] oppure la presenza del consenso esplicito dell'interessato;[50] quest'ultimo, in particolare, viene menzionato in riferimento ad applicazioni co-

[39] *Ibid*., considerando 51.

[40] *Ibid*., considerando 71.

[41] *Ibid*., art. 4, n. 15.

[42] Guidelines 04/2020 adopted on 21 April 2020, cit., p. 8.

[43] Article 29 Working Party, Annex to the letter to Paul Timmers – health data in apps and devices – of 5 February 2015, ec.europa.eu.

[44] Statement adopted on 19 March 2020, cit., p. 2; Guidelines 04/2020 adopted on 21 April 2020, cit., p. 8.

[45] Sul punto, si veda O. POLLICINO, F. RESTA, *Data tracing, no a deleghe in bianco all'algoritmo*, in *CorCom*, 24 marzo 2020, www.corrierecomunicazioni.it.

[46] App "Immuni", Informativa Privacy, cit., par. 3.

[47] Guidelines 04/2020 adopted on 21 April 2020, cit., p. 8.

[48] Art. 9, par. 2, lett. h), e art. 9, par. 3, del Regolamento 2016/679, cit.

[49] *Ibid.*, art. 9, par. 2, lett. j).

[50] *Ibid.*, art. 9, par. 2, lett. a).

me la "Corona-Warn-App".[51] Più complesso, invece, far riferimento in questo frangente alla necessità di tutelare un interesse vitale dell'interessato o di un'altra persona fisica: a differenza di quanto visto in precedenza per i dati non sensibili,[52] per i dati sensibili tale base giuridica riguarda solo l'ipotesi in cui "l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso".[53]

Infine, occorre tornare su un concetto che già emerge dall'analisi fin qui svolta nel presente paragrafo, ma che è opportuno puntualizzare meglio: la base giuridica non ha solo la funzione di fornire una giustificazione al trattamento; infatti, a seconda della base giuridica che si individua, ai sensi di quanto previsto dagli artt. 6 e 9 le operazioni di trattamento dovranno rispettare condizioni e limiti diversi. Se, per il trattamento dei dati relativi alla salute, si sceglie la solida base giuridica rappresentata dalla necessità del trattamento per motivi di interesse pubblico nel settore della sanità pubblica, sarà necessario rispettare quanto previsto dall'art. 9, par. 2, lett. i). Di conseguenza, il trattamento dovrà avvenire sulla base del diritto dell'UE o degli Stati membri, che dovrà altresì prevedere "misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale". A titolo esemplificativo, l'Italia, proprio in ossequio a tale previsione, ha inserito una specifica disposizione all'interno del Decreto-Legge 30 aprile 2020, n. 28: si tratta dell'art. 6, dedicato al "Sistema di allerta COVID-19".[54] Allo stesso modo, se come base giuridica si individua il consenso, esso dovrà rispettare tutti i requisiti prescritti all'interno del Regolamento 2016/679, e così via.

IV. I principi che regolano il trattamento: limitazione della finalità, minimizzazione, limitazione della conservazione

Il trattamento dei dati deve poi rispettare numerosi, importantissimi principi.[55] Innanzitutto, è doveroso menzionare il principio di limitazione della finalità, secondo cui i dati personali devono essere "raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità".[56] In ossequio a tale principio le finalità devono essere sufficientemente specifiche, così da escludere trattamenti ulteriori per scopi non correlati alla gestione della crisi sanitaria causata da COVID-19: ad esempio, trattamenti per fini commerciali o per le attività di contrasto di matrice giudiziaria o di poli-

[51] "Corona-Warn-App", *Privacy Notice*, cit., par. 3.

[52] Art. 6, par. 1, lett. d), del Regolamento 2016/679, cit.

[53] *Ibid.*, art. 9, par. 2, lett. c).

[54] Art. 6 del Decreto-Legge 30 aprile 2020, n. 28, recante Misure urgenti per la funzionalità dei sistemi di intercettazioni di conversazioni e comunicazioni, ulteriori misure urgenti in materia di ordinamento penitenziario, nonché disposizioni integrative e di coordinamento in materia di giustizia civile, amministrativa e contabile e misure urgenti per l'introduzione del sistema di allerta Covid-19.

[55] Su tali principi, si veda più diffusamente G. Comandé, G. Malgieri (a cura di), *Manuale per il trattamento dei dati personali*, cit., p. 16 *et seq*.

[56] Art. 5, par. 1, lett. b), del Regolamento 2016/679, cit.

zia.[57] Sarà dunque essenziale definire con chiarezza la finalità, e successivamente garantire che l'uso dei dati personali sia necessario e proporzionato rispetto alla stessa.

Occorre poi citare il principio di minimizzazione: si tratta di una diretta conseguenza del principio di finalità, in base al quale i dati in questione devono essere "adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati"[58] e, dunque, non superflui, inutili o sovrabbondanti.[59] In ragione di tale principio, l'applicazione di tracciamento non dovrà raccogliere informazioni non correlate o non necessarie come, per esempio, dati anagrafici, identificativi di comunicazione, voci di directory del dispositivo, messaggi, registrazioni di chiamate, dati relativi all'ubicazione o identificativi del dispositivo. Quindi, i dati trasmessi dall'app dovranno includere solo identificatori univoci e pseudonimi, generati dall'app e specifici della stessa, i quali dovranno essere rinnovati regolarmente in modo da limitare il rischio di identificazione e localizzazione fisica delle persone.[60] A titolo esemplificativo, proprio per rispettare tale principio, il già citato Decreto-Legge italiano del 30 aprile prevede che "i dati personali raccolti dall'applicazione [...] siano esclusivamente quelli necessari ad avvisare gli utenti dell'applicazione di rientrare tra i contatti stretti di altri utenti accertati positivi al COVID-19";[61] che "il trattamento effettuato per allertare i contatti sia basato sul trattamento di dati di prossimità dei dispositivi, resi anonimi oppure, ove ciò non sia possibile, pseudonimizzati; è esclusa in ogni caso la geolocalizzazione dei singoli utenti";[62] e che "siano garantite [...] misure adeguate ad evitare il rischio di reidentificazione degli interessati cui si riferiscono i dati pseudonimizzati oggetto di trattamento".[63] In ragione di quanto esposto, inoltre, è possibile affermare che le app che si avvalgono della tecnologia *Bluetooth*, come le citate "Immuni", "Corona-Warn-App", "Stop Covid" e "Stopp Corona", sono più rispettose del principio di minimizzazione e dunque preferibili sul piano della protezione dei dati rispetto a quelle che si avvalgono della localizzazione GPS,[64] come l'app slovacca "Zostaň zdravý", l'app cipriota "CovTracer" e l'app bulgara "ViruSafe".[65] Ciò è affermato anche dall'EDPB, secondo cui le *contact tracing apps* non necessitano del tracciamento della posizione dei singoli utenti e sarebbe dunque più opportuno utilizzare i dati di prossimità[66], generati dallo scambio di segnali *Bluetooth*.

Sempre a parere dell'EDPB, inoltre, nonostante nella conservazione dei dati sia astrattamente praticabile tanto l'approccio centralizzato quanto quello decentralizzato,

[57] Guidelines 04/2020 adopted on 21 April 2020, cit., p. 7.
[58] Art. 5, par. 1, lett. c), del Regolamento 2016/679, cit.
[59] G. COMANDÉ, G. MALGIERI (a cura di), *Manuale per il trattamento dei dati personali*, cit., pp. 18-19.
[60] Guidelines 04/2020 adopted on 21 April 2020, cit., p. 9.
[61] Art. 6, co. 2, lett. d), del Decreto-Legge 30 aprile 2020, n. 28, cit.
[62] *Ibid*., art. 6, co. 2, lett. c).
[63] *Ibid*., art. 6, co. 2, lett. d).
[64] S. ROSSELLO, P. DEWITTE, *Anonymization by decentralization?*, cit.
[65] A. TOMASCHEK, *Comparing Contact Tracing Apps*, cit.
[66] Guidelines 04/2020 adopted on 21 April 2020, cit., p. 7.

quest'ultimo sarebbe maggiormente conforme al principio di minimizzazione:[67] seguendo un simile modello è infatti possibile comunque conseguire la finalità di allertare chi ha avuto un contatto a rischio con una persona infetta, ma fornendo al server il minor numero possibile di dati.[68] In tale ottica, dunque, la soluzione adottata per l'app italiana, per quella tedesca e per quella austriaca appare preferibile rispetto a quella scelta per l'app francese "Stop Covid".[69]

Concludendo sui principi che regolano il trattamento, un'altra diretta emanazione del principio di finalità è il principio di limitazione della conservazione,[70] secondo cui i dati personali devono essere "conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati".[71] In virtù di quest'ultimo, la conservazione dovrà essere limitata in base alle reali esigenze e alla rilevanza medica dei dati personali, tenendo conto anche di fattori di natura epidemiologica come ad esempio il periodo di incubazione del virus: successivamente, tutti i dati personali dovranno essere cancellati o resi anonimi.[72] Da questo punto di vista, menzionando ancora una volta come esempio il Decreto-Legge italiano, è previsto che "i dati relativi ai contatti stretti siano conservati, anche nei dispositivi mobili degli utenti, per il periodo strettamente necessario al trattamento [...]; i dati sono cancellati in modo automatico alla scadenza del termine",[73] e anche che tutti i dati personali trattati devono essere cancellati o resi definitivamente anonimi comunque non oltre il 31 dicembre 2020.[74]

V. Diritti dell'interessato e responsabilità del titolare del trattamento

Non bisogna poi dimenticare che la persona i dati della quale vengono trattati deve essere posta in condizione di esercitare i suoi diritti, elencati nel Capo III del Regolamento 2016/679. In primo luogo, in conseguenza del principio di trasparenza,[75] l'interessato ha diritto di ricevere tutta una serie di informazioni; inoltre, deve essere posto nelle condizioni di esercitare gli altri diritti, come l'accesso, la rettifica o la cancellazione. Sempre a titolo esemplificativo, il Decreto-Legge 30 aprile 2020, n. 28, prevede innanzitutto che "gli utenti ricevano, prima dell'attivazione dell'applicazione, ai sensi degli artt. 13 e 14 del Regolamento 2016/679, informazioni chiare e trasparenti al fine di raggiungere una

[67] *Ibid*., p. 9.

[68] S. Rossello, P. Dewitte, *Anonymization by decentralization?*, cit.

[69] Vrije Universiteit Brussel – Law, Science, Technology & Society Research Group, *Contact Tracing Apps*, cit.

[70] G. Comandé, G. Malgieri (a cura di), *Manuale per il trattamento dei dati personali*, cit., p. 19.

[71] Art. 5, par. 1, lett. e), del Regolamento 2016/679, cit.

[72] Guidelines 04/2020 adopted on 21 April 2020, cit., p. 8.

[73] Art. 6, co. 2, lett. e), del Decreto-Legge 30 aprile 2020, n. 28.

[74] *Ibid*., art. 6, co. 6.

[75] Art. 5, par. 1, lett. a), del Regolamento 2016/679, cit.

piena consapevolezza, in particolare, sulle finalità e sulle operazioni di trattamento, sulle tecniche di pseudonimizzazione utilizzate e sui tempi di conservazione dei dati";[76] poi che "i diritti degli interessati di cui agli articoli da 15 a 22 del Regolamento (UE) 2016/679 possano essere esercitati anche con modalità semplificate".[77]

Deve poi essere definita chiaramente la titolarità del trattamento dell'app di tracciamento dei contatti.[78] Il titolare, ai sensi del principio di responsabilizzazione o "*accountability*",[79] deve mettere in atto le misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento. Inoltre, deve adempiere agli obblighi del Capo IV, come quello di effettuare una valutazione d'impatto, che scatta in presenza di un "rischio elevato" per i diritti e le libertà delle persone fisiche;[80] tale condizione, nel caso di specie, parrebbe integrata, visto che il trattamento riguarda dati relativi alla salute (e dunque sensibili), che l'adozione è prevista su larga scala, che comporta un monitoraggio sistematico e che è previsto l'utilizzo di una nuova soluzione tecnologica.[81] Portando, per un'ultima volta, il Decreto-Legge italiano come esempio, si può notare come il titolare del trattamento venga individuato nel Ministero della salute,[82] e si menziona anche l'obbligo di effettuare la valutazione d'impatto.[83]

Infine, sempre in tema di rischi, occorre ricordare che anche sotto tale profilo il modello decentralizzato di conservazione dei dati appare astrattamente preferibile rispetto a quello centralizzato. Adottando quest'ultimo, infatti, appare particolarmente problematica l'eventualità di un cyber-attacco al server centrale:[84] la compromissione di tale server determinerebbe la compromissione dell'intero sistema.[85] Tuttavia, come specificato dall'EDPB, anche l'approccio centralizzato è praticabile, a condizione che siano in vigore appropriate misure di sicurezza;[86] secondo il GDPR, infatti, queste ultime devono essere adeguate rispetto al rischio corso.[87]

[76] Art. 6, co. 2, lett. a), del Decreto-Legge 30 aprile 2020, n. 28.
[77] *Ibid*., art. 6, co. 2, lett. f).
[78] Guidelines 04/2020 adopted on 21 April 2020, cit., p. 7.
[79] Art. 24 del Regolamento 2016/679, cit.
[80] *Ibid,*, art. 35.
[81] Guidelines 04/2020 adopted on 21 April 2020, cit., pp. 8-9.
[82] Art. 6, co. 1, del Decreto-Legge 30 aprile 2020, n. 28.
[83] *Ibid*., art. 6, co. 2.
[84] Norton Rose Fulbright, *Contact tracing apps in France*, 5 giugno 2020, www.nortonrosefulbright.com.
[85] S. Rossello, P. Dewitte, *Anonymization by decentralization?*, cit.
[86] Guidelines 04/2020 adopted on 21 April 2020, cit., p. 9.
[87] Art. 32 del Regolamento 2016/679, cit.

VI. Considerazioni conclusive

Le "*contact tracing apps*", il cui utilizzo non rappresenta certo una novità nella lotta contro le epidemie umane,[88] possono essere un importante strumento anche nel contenimento della pandemia da COVID-19. Ovviamente, tali applicazioni non possono sostituire il tracciamento manuale dei contatti effettuato da personale sanitario pubblico qualificato. Solo tale personale potrà meglio valutare con quale probabilità un contatto ravvicinato abbia dato luogo alla trasmissione del virus: in caso di interazione con una persona dotata di adeguato equipaggiamento, ad esempio, il contagio può risultare più difficile. Inoltre, solo la sorveglianza da parte di operatori qualificati può limitare il verificarsi di falsi positivi e negativi.[89] Tuttavia, le app di tracciamento possono svolgere una funzione di supporto e costituire un tassello significativo nell'ambito di una strategia globale in materia di sanità pubblica per combattere la pandemia.[90]

Orbene, in un simile contesto il Regolamento 2016/679 si dimostra uno strumento sensibile alle moderne esigenze,[91] permettendo agli Stati membri di avvalersi di tali applicazioni; queste ultime, tuttavia, devono rispettare varie condizioni al fine di proteggere i dati personali degli utenti. Innanzitutto, è necessario individuare un'idonea base giuridica che giustifichi il trattamento e osservare i limiti che la scelta di tale base giuridica comporta. In secondo luogo, occorre rispettare principi come quelli di limitazione della finalità, di minimizzazione e di limitazione della conservazione. Infine, gli interessati devono essere posti in condizione di esercitare una serie di diritti, mentre il titolare deve adottare misure tecniche e organizzative adeguate al rischio. Nel dettare tali condizioni, il GDPR dà quindi importanti indicazioni utili alla concreta predisposizione delle app in questione: ad esempio, occorre notare che le app che si avvalgono della tecnologia *Bluetooth* (come quelle di Italia, Germania, Francia e Austria) sono più rispettose del principio di minimizzazione rispetto alle app che utilizzano la localizzazione GPS (come quelle di Slovacchia, Cipro e Bulgaria). Inoltre, alla luce del medesimo principio, nonché per ragioni di sicurezza, le applicazioni che adottano un approccio decentralizzato di conservazione dei dati sono preferibili rispetto a quelle che optano per un modello centralizzato, come l'app francese "Stop Covid".

In definitiva, il GDPR opera un bilanciamento tra le esigenze di interesse pubblico nel settore della sanità e quelle di protezione dei dati, dettando un criterio di gradualità:[92] occorre innanzitutto testare l'efficacia di misure meno invasive e incrementarle esclusivamente nel caso in cui esse non siano in grado di raggiungere le finalità prefis-

[88] G.M. Ruotolo, *Alcune osservazioni sulle app di tracciamento dei contatti e dei contagi alla luce del diritto dell'Organizzazione mondiale del commercio*, in *SIDIBlog*, 13 maggio 2020, www.sidiblog.org.

[89] Guidelines 04/2020 adopted on 21 April 2020, cit., p. 8.

[90] *Ibid*., p. 4.

[91] E.M. Kuşkonmaz, E. Guild, *Covid-19: A New Struggle over Privacy, Data Protection and Human Rights?*, in *European Law Blog*, 4 maggio 2020, europeanlawblog.eu.

[92] O. Pollicino, F. Resta, *Data tracing*, cit.

sate.[93] Solo seguendo tale approccio, infatti, è possibile generare un clima di fiducia da parte degli utenti e creare le condizioni per l'accettabilità sociale delle applicazioni, da cui dipende la piena efficacia delle misure stesse.[94]

[93] G. Della Morte, *La tempesta perfetta COVID-19, deroghe alla protezione dei dati personali ed esigenze di sorveglianza di massa*, in *SIDIBlog*, 30 marzo 2020, www.sidiblog.org.

[94] Guidelines 04/2020 adopted on 21 April 2020, cit., p. 3.