Pandemia, Immuni e app di tracciamento tra GDPR ed evoluzione del ruolo dei Garanti

Francesco Pizzetti

1. Uno degli effetti più evidenti dell'epidemia provocata dal Covid-19 nel corso di questo anno è stato certamente quello di obbligare milioni di persone a misurarsi con la società digitale e con le opportunità, ma anche con i pericoli, che essa presenta rispetto ai servizi che mette a disposizione delle nostre società.
Per contro è chiaro a tutti che da questo punto di vista l'epidemia è un vero *turning point*, delle cui conseguenze oggi non abbiamo ancora adeguata consapevolezza.
È in questo quadro che, a me pare, il dibattito molto ampio svoltosi in questi mesi, in particolare Italia, sulla app Immuni deve essere collocato.
Al di là della legittimità del sistema di *tracing* proposto e, in particolare, della sua compatibilità con la normativa in materia di privacy, questo dibattito ha "sdoganato" nell'immaginario collettivo alcune prospettive, anche legate a specifiche tecnologie, delle quali fino a qualche mese fa pochi, fra il grande pubblico degli utenti del web, avevano consapevolezza.
Sul piano tecnologico l'aspetto più importante è stato quello di mettere tutti al corrente che i sistemi di *tracing*, intesi come sistemi che consentono il tracciamento dei devices, e in particolare degli smartphone, si dividono in sistemi accentrati e decentrati. La differenza tra le due famiglie di sistemi riguarda se i dati di tracciamento o quelli destinati a consentirlo in caso di bisogno, sono accentrati, ovvero conservati in una specifica struttura alla quale tutti i dati generati dai telefonini che entrano tra loro in contatto pervengono; o decentrati, ovvero conservati sugli stessi devices telefonici e analizzati ai fini di rilevare i contatti solo laddove ne sorga la necessità. Entrambi i sistemi possono superare lo scoglio di dover fare ricorso in via generale a tecniche di geolocalizzazione che, come tali, suscitano problemi di particolare rilievo, specialmente rispetto all'individuazione di chi abbia titolo per accedere a tali dati e trattarli, e quindi anche per quanto riguarda più da vicino la tutela dei dati personali relativi.
Di non minore importanza è stato anche rendere ampiamente diffusa la conoscenza della possibilità di fare in modo che i devices dialoghino tra loro attraverso la tecnologia Bluetooth, che consente ai devices stessi di trasmettersi l'un l'altro codici identificativi che attestano il fatto che i due strumenti si sono trovati in un ambito spaziale coincidente con quello, molto limitato, che i sistemi basati su questa tecnologia consentono di utilizzare, registrando anche il tempo durate il quale tale contatto è durato e la distanza alla quale è avvenuto. I dati relativi, se il sistema è decentrato, restano sui rispettivi devices, diminuendo così molto i rischi derivanti dalla loro concentrazione in un unico sito al quale sia possibile accedere, potendo venire così facilmente a cono-

scenza in modo illecito di un numero potenzialmente molto elevato di dati personali, quali sono quelli prodotti da devices riconducibili a utenti specifici, venuti in contatto tra loro. La compresenza di due devices nel raggio di azione compatibile con la tecnologia Bluetooth consente infatti, a sua volta, un tracciamento molto accurato della prossimità dei due strumenti e del tempo nel quale tale contatto è avvenuto, consentendo così di tracciare i contatti tra le persone alle quali i devices sono riconducibili.
Dal punto di vista giuridico, l'adozione di tecnologie di tracciamento dei contatti tra le persone (o dei devices usati dalle persone) è stata caldamente raccomandata, in particolare anche dalla Organizzazione Mondiale della Sanità, proprio al fine di combattere il contagio. La conoscenza degli avvenuti contatti in un raggio limitato e per un tempo definito può infatti consentire maggiore rapidità di interventi curativi da parte delle strutture sanitarie che siano messe al corrente del contatto. Di conseguenza è possibile accertare più rapidamente se si è verificato o no il contagio e gli interventi curativi possono avere maggiore efficacia, così come possono essere più efficaci le misure di contenimento del contagio. Per queste ragioni il ricorso a queste tecnologie è stato considerato particolarmente raccomandabile nell'ambito internazionale, e soprattutto il ricorso ad esse è stato suggerito dall'OMS, come uno strumento particolarmente efficace di lotta all'epidemia.
Sulla base di questi aspetti è stato possibile allo EDPB e, di conseguenza, ai singoli Garanti europei, superare con una certa agevolezza il tema del rapporto tra l'utilizzazione di queste tecnologie e la normativa a tutela dei dati personali, anche con riguardo a dati che, come nel caso, si riferiscono alla salute delle persone entrate tra loro in contatto.
È stato possibile, infatti, fare ricorso all'art. 9, lett. *i*), del GDPR, secondo il quale il trattamento di dati relativi alla salute è legittimo quando «è dichiarato necessario per motivi di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni o le garanzie del paragrafo 3».
Il par. 3 dell'art. 9, a sua volta, specifica che la lett. *h*) del primo paragrafo consente la legittimità dei trattamenti se «i dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite da o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti».
Proprio all'art. 9 del GDPR hanno fatto riferimento le Autorità garanti che, riunite nello EDPB, hanno confermato con un documento contenente Linee guida chiare e ben scritte la posizione già assunta dalla Presidente Andrea Jelinek in più occasioni (fra le quali merita segnalare la lettera a Olivier Micol Capo della Unit European Commission DG for Justice and Consumers) e sulle indicazioni già formulate in varie occasioni dalle Autorità garanti nazionali, tra le quali anche la CNIL e il Garante italiano.
Essendo tutti documenti ben noti e ormai già citati in molte sedi sarà sufficiente qui richiamarne gli aspetti essenziali contenuti nelle Linee guida 04/2020 dello EDPB che consistono in alcuni punti molto chiari e molto fermi.

Il primo punto ribadisce che la tutela dei dati personali, conformemente all'art. 8 della Carta dei diritti fondamentali dell'UE, adottata con rango di trattato nel Trattato di Lisbona, è un diritto fondamentale della persona, come tale riconosciuto dall'Unione Europea. Ne consegue tuttavia che, pur essendo un diritto fondamentale, esso è comprimibile quando ciò sia necessario per tutelare altri non meno importanti diritti fondamentali riconosciuti come tali anche dalla medesima Carta. Non a caso nel parere dello EDPB si ripete, anche sulla traccia di una ormai consolidata giurisprudenza costituzionale fatta propria sia dalla Corte di giustizia che da molte Corti costituzionali degli Stati UE, che nell'ambito dei diritti fondamentali non può esservi alcun "diritto tiranno" la cui osservanza possa giustificare la compressione, anche fino all'annullamento, di altri diritti, parimenti fondamentali.

Del resto, questo costituisce anche la base dello stesso art. 9 del GDPR il quale, tuttavia, subordina il bilanciamento tra la tutela dei dati personali e altri diritti fondamentali che possano essere in gioco al verificarsi di una delle situazioni di cui dalla lett. *a*) alla lett. *j*) del suo par. 2.

Ovviamente il prodursi di una delle situazioni di cui alla norma citata implica il sorgere di una causa di legittimità del trattamento, in assenza della quale (o delle quali) il trattamento dei dati, a cominciare dalla loro raccolta, è da considerarsi illecito e dunque vietato. Peraltro, il sorgere di tale causa di legittimazione si limita, quanto agli effetti, ad autorizzare il decisore UE o i decisori nazionali ad effettuare il necessario bilanciamento tra il diritto alla protezione dei dati personali e gli altri diritti fondamentali in gioco, al fine di assicurare garanzie adeguate a tutti i diritti e agli interessi fondamentali dell'interessato.

Se si riflette attentamente sulle cause in presenza delle quali è considerata legittima la compressione del diritto alla tutela dei dati personali si può agevolmente constatare che pressoché tutte riguardano la tutela della persona alla quale si riferiscono i dati.

Tale riserva è evidentemente posta a tutela della persona, e costituisce quasi un aspetto essenziale della sua libertà, ben più che della sua "dignità". Non a caso la prima causa di legittimità della compressione della tutela dei dati personali, quella posta all'inizio del par. 2 dell'art. 9 del GDPR e indicata alla lett. *a*), consiste nel consenso dato dall'interessato stesso.

Il "consenso" è nel quadro della protezione dati di matrice europea lo strumento principale attraverso il quale l'interessato può esprimere la propria volontà e tutelare autonomamente la propria libertà personale nel mondo dei trattamenti dei dati che lo riguardano. Ovviamente l'esercizio del consenso è legato alla completezza dell'informativa che, non a caso, è oggetto di ben due articoli, il 13 e il 14, e che il GDPR vuole sia completa, chiara, ed espressa in linguaggio semplice e comprensibile da tutti, nel rispetto del principio di trasparenza al quale è dedicata tutta la Sezione I del Capo III del GDPR.

La stessa centralità della persona interessata è alla base anche delle altre ipotesi di restrizione della tutela dei dati personali.

È questa infatti la ragione della legittimità dei trattamenti di dati personali anche senza il consenso dell'interessato nei casi in cui questi trattamenti:

a. siano funzionali a consentire all'interessato di assolvere agli obblighi ed esercitare

i diritti specifici del titolare o dell'interessato in materia di diritto del lavoro, della sicurezza sociale e della protezione sociale, sempre che ciò sia previsto dal diritto dell'Unione o dal diritto nazionale e siano definite le garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato (art. 9, par. 2, lett. *b*);

b. siano necessari a tutelare interessi vitali dell'interessato o altra persona fisica e l'interessato non sia in grado di esprimere il proprio consenso (art. 9, par. 2, lett. *c*);
c. il trattamento avvenga nell'ambito di una associazione o fondazione che, senza scopo di lucro, persegua finalità politiche, filosofiche, religiose o sindacali, concorrendo così a rendere attivi altri diritti fondamentali riconosciuti alla persona, e anche in questi casi comunque operando con adeguate garanzie (art. 9, par. 2, lett. *d*);
d. il trattamento riguardi dati personali resi pubblici dall'interessato (art. 9, par. 2, lett. *e*);
e. il trattamento è necessario per difendere in sede giudiziaria diritti dell'interessato (art. 9, par. 2, lett. *f*);
f. il trattamento è necessario per motivi di interesse pubblico rilevanti, che devono però essere individuati dal diritto dell'Unione o degli Stati membri in un quadro che assicuri la proporzionalità tra la compressione della tutela e le finalità perseguite, prevedendo inoltre misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato (art. 9, par. 2, lett. *g*);
g. il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sociali sulla base del diritto dell'Unione o degli Stati membri, ovvero sulla base di un contratto con un professionista della sanità, o, ancora, sia conforme alle nome stabilite da organismi competenti di diritto dell'Unione o degli altri membri della sanità (art. 9, par. 2, lett. *h*) sempre che i dati personali siano trattati sotto la responsabilità di un professionista soggetto al segreto professionale ovvero per le gestione di sistemi o servizi sanitari o sociali conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o degli Stati membri (art. 9, par. 3, richiamato dall'art. 9, par. 2, lett. *h*);
h. il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati che, anche in questi casi, devono prevedere misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale (art. 9, par. 2, lett. *i*);
i. infine, la protezione dei dati personali può trovare compressioni per finalità di archiviazione nel pubblico interesse, di ricerca scientifica o a fini statistici in conformità all'art. 89, par. 1 del GDPR. Anche in questo caso, comunque, ciò deve avvenire «sulla base del diritto dell'Unione o nazionale che, a sua volta, deve essere proporzionato alle finalità perseguite, rispettare l'essenza del diritto alla protezione dei dati personali e prevedere misure appropriate e specifiche per tutelare i diritti e gli interessi dell'interessato» (art. 9, par. 3, lett. *j*).

In sostanza, se si legge con attenzione, lungimiranza, e capacità di visione prospettica l'art. 9, par. 2, del GDPR si vede con facilità che le ragioni per cui le regole relative alla tutela dei dati personali possono essere compresse riguardano due grandi categorie di casi e situazioni.

La prima, a carattere generale e perfettamente coerente con l'impianto complessivo del GDPR, è il consenso dell'interessato di cui all'art. 9 par. 1, lett. *a*) che ribadisce la sovranità della persona sui suoi dati, sia nel senso che il loro uso è legittimo solo col consenso dell'interessato sia nel senso che a tal fine l'interessato ha diritto a una informativa chiara e comprensibile che gli consenta tanto di esprimere un consenso libero e informato quanto di esercitare eventualmente il diritto a ritirarlo nel tempo.

La seconda linea è che il consenso è, in via generale, necessario solo ove i trattamenti abbiano finalità di tutela dell'interessato sia rispetto alla sua vita che alla tutela dei suoi diritti. In entrambe queste due prospettive è evidente la centralità della tutela della persona interessata che per un verso è strettamente connessa alla condizione del consenso, e quindi di una specifica manifestazione di volontà non condizionata né condizionabile e sempre revocabile, ovvero alla necessità di tutelare diritti e interessi dello stesso interessato.

Tuttavia, però, quando una di queste due prospettive non ricorra, e siano presenti invece ragioni di restrizione della tutela connesse all'interesse pubblico, sia esso di natura sanitaria o connessa alla salute collettiva o di natura statistica e conoscitiva, allora è sempre necessario l'intervento del legislatore unionale o statale.

Non solo: sulla base del testo delle norme citate è chiaro che la legittimità di una compressione della tutela dei dati personali non basata sul consenso ma sull'intervento unionale o statale relativo a una delle situazioni appena richiamate richiede sempre implicitamente una attenta valutazione dei diversi diritti in gioco, ed è legittima in quanto per un verso il decisore unionale o statale abbia ragione di ritenere, all'esito del bilanciamento, che sussistano ragioni adeguate alla compressione della tutela dei dati personali che devono essere collegate inevitabilmente alla tutela di altri diritti parimenti fondamentali. Inoltre, tutte le norme contenute nell'art. 9 che prevedono l'intervento unionale o statale stabiliscono con chiarezza che non basta un bilanciamento fra i diversi interessi e diritti in gioco che giustifichi tale compressione, ma che è necessario anche che il decisore unionale o statale adottino misure appropriate e specifiche per tutelare tutti i diversi diritti fondamentali in gioco, ivi compreso ovviamente il diritto alla tutela dei dati personali dell'interessato.

Non basta dunque una valutazione relativa ai diversi diritti fondamentali in gioco per giustificare la compressione della tutela ma occorre anche adottare, se necessario, ulteriori e nuove misure normative che assicurino la tutela dei diritti e degli interessi fondamentali dell'interessato.

Dunque, stando all'art. 9 del GDPR, appare chiaro che l'intervento del legislatore unionale o statale non può limitarsi a definire e circoscrivere le limitazioni della tutela dei dati personali relativamente a casi specifici e in rapporto ad altri diritti fondamentali ma deve indicare anche le forme di tutela dei dati personali, e in generale dei diritti fondamentali delle persone, adeguate ad assicurare che le compressioni relative alle norme generali adottate non pregiudichino comunque la tutela dei diritti fondamentali

e degli interessi dell'interessato.
Va da sé che nella logica dell'art. 9 questo implica anche che le scelte fatte dal decisore unionale o nazionale relative alla compressione della tutela generale e all'adozione di forme alternative di tutela dei diritti fondamentali possano essere soggette anche a un controllo giurisdizionale, rimesso alla Corte di giustizia, per quanto riguarda le decisioni unionali, e alle Corti nazionali, sulla base dell'ordinamento costituzionale interno di ciascun Stato membro, tenuto conto della competenza della Corte di Giustizia dell'Unione, per quanto riguarda le decisioni statali.

2. Merita inoltre sottolineare che il GDPR contiene anche una altra disposizione che ben avrebbe potuto essere utilizzata per giustificare interventi unionali o statali di limitazione della normativa a tutela dei dati personali e che, invece, non è mai stata presa in specifica considerazione nell'ambito relativo alla valutazione della compatibilità dell'utilizzazione di app di tracciamento rispetto al GDPR e a quanto in esso previsto. Il riferimento è all'art. 23 del GDPR stesso, che contiene in via generale la disposizione relativa, come specifica il titolo della norma, le "limitazioni" al GDPR, soprattutto con riguardo agli artt. da 12 a 22 e 34 nonché all'art. 5 (cfr. art. 253, par. 1). Il richiamo alla sostanziale trascuratezza di questa norma da parte dei Garanti è in questa sede importante sia perché merita sottolineare la rinuncia a richiamare anche tale articolo sia perché proprio tale rinuncia sembra ribadire il sostanziale interesse dello EDPB (e anche dei Garanti nazionali) a non sollecitare l'intervento del decisore unionale e di quelli nazionali.
Pare infatti chiaro che l'intervento del decisore unionale o statale anche nei casi dell'art. 23 ha lo scopo, pur non sottolineato con la stessa forza di quanto si fa nell'art. 9, di garantire che spetti ai decisori in questione sia verificare la necessità e, soprattutto, la ragionevolezza delle limitazioni rispetto ai tipi di trattamento e alle loro finalità sia individuare le eventuali garanzie adottabili per assicurare comunque la tutela del diritto alla protezione dei dati personali pur in un quadro di restrizione della normativa generale in materia.
Dunque, l'eventuale ed esplicito richiamo a tale articolo avrebbe ragionevolmente dovuto spingere sia i Garanti che lo EDPB a subordinare la legittimità della eventuale compressione delle norme in materia di tutela dei dati personali a un esplicito intervento del decisore unionale o nazionale, tanto ai sensi dell'art. 9 che dell'art. 23 del GDPR.
Questo non è avvenuto, malgrado che l'art. 9 sia stato ampiamente citato. Ed è proprio questo che impone di porsi alcuni degli interrogativi qui esaminati.

3. Il problema centrale è che sia le lettere della Presidente dello EDPB Andrea Jelinek, sia le Linee guida 04/2020 sull'uso dei dati di localizzazione per il tracciamento dei contatti nel contesto dell'emergenza legata al Covid-19, pur richiamando ampiamente in via generale le norme del GDPR, e in particolare, tra quelle qui citate l'art. 9, non vincolano affatto la legittimità della adozione delle app di tracciamento per combattere l'epidemia a specifiche previsioni normative dell'UE o degli Stati membri né tengono fermo il consenso come unica, o prevalente, causa di legittimità dei tratta-

menti anche in assenza di specifiche previsioni o di esigenze legate alla tutela dei diritti dell'interessato.
Il punto "forte" del Parere dello EDPB riguarda essenzialmente il condizionare la legittimità dell'uso di app di tracciamento, anche per finalità di lotta all'epidemia, al fatto che non sia reso in alcun modo obbligatorio o vincolato il loro scaricamento e il loro uso da parte degli utenti di telefonia mobile o comunque da parte dei cittadini interessati.
Si specifica, anzi, esplicitamente che in tanto l'uso di queste app (nel caso italiano di Immuni) è legittimo in quanto il loro uso implichi la libera scelta da parte degli utenti di smartphone in ordine alla decisione se scaricarle o meno e se farne o meno uso.
Si chiede poi che il sistema sia almeno interoperabile a livello di tutti gli Stati della UE e che le modalità di attuazione siano in grado di garantire la necessaria coerenza tra dati usati e tipologia di trattamenti e finalità che si vogliono raggiungere. Si chiede inoltre, in coerenza, con quanto previsto dall' art. 9, par. 2, lett. *h*), che i trattamenti dei dati sanitari siano posti in essere da professionisti della sanità, vincolati al rispetto delle norme sul segreto professionale oltre che dotati della competenza sanitaria necessaria a decidere sulla necessità dei trattamenti stessi.
Inoltre sia nelle Linee guida citate che nei pareri successivamente espressi, soprattutto dai Garanti nazionali, rispetto a specifiche app adottate nel territorio degli Stati membri (per l'Italia cfr. Garante privacy, *Provvedimento di autorizzazione al trattamento dei dati personali effettuato attraverso il Sistema di allerta Covid-19-App Immuni* (doc. web n. 9356568) del 1 giugno 2020) si specifica che se queste condizioni sono rispettate l'uso di applicazioni di tracciamento per finalità di lotta all'epidemia Covid-19 sono compatibili con la normativa di protezione dei dati personali.
Ovviamente ciascuno degli aspetti richiamati meriterebbe una analisi specifica, e certo colpisce che da un lato si chieda che la decisione se scaricare o no l'app sia rimessa unicamente agli utenti, pur sapendo che il numero di app effettivamente scaricate ed effettivamente funzionanti è elemento condizionante circa la probabilità di raggiungere le finalità che il sistema di cui la app fa parte e il suo uso si propongono e dall'altro si insista nel considerare, giustamente, condizione essenziale di legittimità dell'uso della app la coerenza con le finalità che con la sua utilizzazione si vogliono raggiungere.
In questa sede, però, merita richiamare l'attenzione su un altro aspetto delle Linee guida che a prima vista può sfuggire e, di fatto, sembra essere sfuggito in generale a tanti commentatori sia della tecnologia legata all'app Immuni che delle posizioni dei Garanti di protezione dei dati personali, Garante italiano compreso.

4. Il punto essenziale della posizione assunta dalle Autorità di protezione dei dati personali nelle Linee guida 04/2020 e già espresse anche nello Statement della Presidente dello EDP Andrea Jelinek del 16 marzo 2020, è infatti che, pur rinviando alle norme del GDPR che richiedono l'intervento dei decisori unionali e nazionali per consentire limitazioni della tutela dei dati personali al fine di assicurare adeguate garanzie per tutti i diritti e gli interessi fondamentali in gioco, esse sembrano accentuare la loro attenzione quasi esclusivamente sulla libertà (o se si preferisce la non obbligatorietà della scelta se avvalersi o meno di questa app).

Peraltro le Linee guida aggiungono anche altre specificazioni, legate essenzialmente alla necessità che, per assicurare il raggiungimento della finalità dichiarata, il sistema adottato da uno Stato sia compatibile e interoperabile con quelli adottati in altri Stati, in ragione del fatto che, come dicono specificamente anche le Linee guida, l'epidemia e i virus non conoscono frontiere e che comunque le modalità di funzionamento delle app adottate in ciascun Paese assicurino una ragionevole raggiungibilità delle finalità che la giustificano.

Inoltre, le Linee guida ricordano la necessità che sia garantito il rispetto dei principi di *privacy by design* e *by default*; una idonea valutazione di impatto di rischio; misure di sicurezza adeguate in ordine al funzionamento complessivo dei trattamenti, coerenti con i rischi che questi comportano e con la delicatezza dei dati trattati.

Su questi ultimi aspetti, rigorosamente richiamati anche dal Garante italiano, non si può che esprimere apprezzamento, così come non si può non apprezzare che il Garante italiano, chiamato a esprimersi sulla compatibilità di Immuni con il quadro europeo e nazionale di protezione dei dati personali, col Provvedimento del 1 giugno 2020 recante "autorizzazione al trattamento dei dati personali effettuato attraverso il Sistema di alert Covid-19-App Immuni" del 1 giugno 2020, abbia dedicato specifica attenzione proprio anche a questi aspetti, sottolineando in particolare la adeguatezza della DPIA presentata dal Governo e relativa alla app Immuni, compreso l'uso della piattaforma Google/Apple, nel frattempo resa disponibile dalle due multinazionali (cfr. Provvedimento citato, punto 7). Merita inoltre sottolineare che proprio rispetto al contenimento dei rischi e al contenuto della DPIA, il Provvedimento citato contiene importanti ulteriori indicazioni di cui al punto 7.3, con particolare riguardo alla conservazione, alla protezione e alla finale cancellazione dei dati, giungendo anche a specificare le misure da adottare rispetto agli amministratori di sistema e dando tempo trenta giorni al Ministero della salute per comunicare le misure adottate.

Tuttavia, pur riconoscendo la attenzione dedicata dal Garante ad adeguarsi alle Linee guida dello EDPB e a definire anche gli ulteriori vincoli appena richiamati, è necessario sottolineare che le modalità con le quali si è operato, sia a livello italiano che europeo rispetto alla valutazione della compatibilità delle app di *tracing* con la legislazione UE sollevano molte perplessità.

Si tratta di aspetti sui quali giova richiamare l'attenzione anche per evitare che l'evoluzione di app di *tracing* possa svilupparsi secondo itinerari palesemente in contrasto con il GDPR e i principi fondamentali della protezione dei dati personali in UE.

Merita osservare, infatti, che il GDPR anche rispetto a quanto previsto nell'art. 9, apre la strada a sistemi di regolazione della tutela dei dati personali "paralleli" rispetto al GDPR (come dimostra il fatto che la norma riguarda casi in cui le regole generali a tutela di questo diritto possono essere "compresse") ma definisce sia i soggetti che alcune modalità essenziali perché ciò possa avvenire e, in particolare, fissa alcuni "paletti" che devono essere rispettati, nel caso che ci interessa in particolare rispetto all'utilizzazione di app a fini di *tracing* degli interessati.

Fra questi paletti, sempre con riguardo all'uso di queste app, vi è innanzitutto la necessaria valutazione del punto di equilibrio ragionevole tra la tutela dei dati personali e quella della tutela di altri diritti della persona, parimenti fondamentali, che potrebbero

essere compromessi dal doveroso e integrale rispetto delle norme di protezione dei dati personali.

Dunque, l'art. 9 entra in gioco proprio quando è necessaria una applicazione della normativa di tutela dei dati personali che, per le modalità con le quali avviene e i criteri che adotta, rispetti e tuteli anche altri diritti fondamentali, altrimenti a rischio.

In secondo luogo va sottolineato che la norma del GDPR prevede obbligatoriamente che tale valutazione sia fatta dal regolatore europeo o nazionale, proprio perché esso, essendo dotato di poteri regolatori, rafforzati da quanto previsto appunto dall'art. 9, può garantire anche una regolazione integrativa che assicuri garanzie e tutele adeguate a tutti i diritti fondamentali in gioco, così come può e deve valutare il corretto punto di equilibrio fra i diversi diritti tra loro in tensione, tenendo conto anche dell'ordinamento costituzionale proprio di ciascun Stato membro che, rispetto a molti diritti, anche fondamentali, varia, sia pure quasi impercettibilmente, da Stato a Stato, e delle regole fondamentali UE con le quali le norme statali formano sistema.

Dunque il quadro disegnato dall'art. 9 ha una sua logica e un suo spessore preciso e profondo: sì alla compressione delle regole di tutela dei dati personali quando siano a rischio altri diritti fondamentali, ma solo a condizione che la compressione avvenga nel rispetto di garanzie appropriate per i diritti fondamentali degli interessati, fra i quali potrebbe essere anche la richiesta di un consenso specifico alla comunicazione dei dati all'esterno del circuito rispetto al quale la raccolta dei dati è consentita in ragione delle sue finalità, come prevede ad esempio l'art. 9, par. 2, lett. *d*).

Così ricostruito il sistema che è alla base di quanto previsto dall'art. 9 del GDPR, si comprende bene perché il potere di consentire la compressione della regolazione generale a tutela dei dati personali sia rimesso solo al decisore UE o a quello degli Stati membri, secondo le regole generali proprie di ciascun Paese.

In sostanza il richiamo al regolatore UE o nazionale come uniche fonti in grado di legittimare trattamenti di dati personali fondati su basi giuridiche diverse da quelle richiamate nell'art. 9 stesso, prima fra tutte il consenso dell'interessato, costituisce a sua volta una ulteriore garanzia delle persone e della tutela dei dati ad esse riferibili.

La valutazione relativa all'equilibrio fra i diversi diritti potenzialmente o concretamente in gioco, infatti, è rimessa ai soli soggetti che possono provvedere adeguatamente non solo a consentire la "restrizione" delle regole del GDPR ma anche ad assicurare, contemporaneamente, garanzie adeguate a tutelare i diritti fondamentali delle persone interessate.

Da questo punto di vista il fatto che *ex* art. 9 i dati personali possano essere trattati anche al di fuori delle regole fondamentali della protezione dei dati personali, prima delle quali il consenso dell'interessato stesso, non è fungibile con l'accertamento fatto dalle Autorità di tutela dei dati personali, proprio perché tali Autorità, pur dotate anche del potere di dettare Linee guida relative alle modalità di attuazione della normativa generale di protezione dati (cfr. art. 57 e, per quanto riguarda lo EDPB, l'art. 70 del GDPR) non hanno però il potere di dettare nuove regole generali derogatorie di quelle contenute nel GDPR.

Dunque, l'eventuale sostituirsi delle Autorità di garanzia (anche riunite nello EDPB) ai regolatori UE o nazionali al fine di consentire o di condizionare "restrizioni" dell'ap-

plicazione delle regole generali del GDPR assicurando tuttavia la tutela di altri diritti fondamentali che potrebbero altrimenti essere compromessi, non appare possibile né compatibile con la regolazione europea nella materia che ci interessa.
Il punto è molto rilevante perché ovviamente indica un limite chiaro ai poteri delle Autorità garanti, che come tali non possono derogare alla normativa di tutela dei dati personali né condizionare la loro attuazione, né autorizzare con i loro provvedimenti una violazione di tali regole.
In questo caso, poi, la sottolineatura è particolarmente necessaria perché di fatto il GDPR non consente alle Autorità garanti, pur dotate di grandi poteri in materia di applicazione di queste norme, di autorizzare o addirittura imporre una loro interpretazione, o attuazione, che sia derogatoria delle norme stesse, soprattutto nel quadro di una normativa che come lo stesso EDPB e la sua Presidente Jelinek hanno ricordato più volte, a tal fine contempla, all'art. 9, la necessità dell'intervento del regolatore UE o di quelli nazionali.

5. Per completare questa riflessione, e renderla anche più equilibrata, merita sottolineare tuttavia che lo EDPB afferma con fermezza e con forza che comunque l'utilizzazione da parte degli utenti di app di tracciamento non può essere imposta per legge ma deve essere rimessa alla libera volontà dei cittadini. Solo ad installazione avvenuta in modo libero e consapevole (sulla base cioè di una informativa completa ed esaustiva circa il funzionamento della app, i dati raccolti, soprattutto se riferiti ai contatti con persone che risultino malate di Coronavirus, possono essere utilizzati dalla app, e da tutto il sistema di tracciamento ad essa collegato anche senza alcun consenso degli interessati. Anche in questo caso, infatti, non è in alcun modo previsto un consenso specifico, e persino l'inserimento dei dati relativi alla salute nel sistema costruito intorno alla app è riservato a operatori sanitari, per rispettare in tal modo almeno quanto previsto dalla lettera i) dell'art. 9 GDPR.
Proprio questa specificazione relativa all'obbligo di riservare al personale sanitario l'inserimento dei dati relativi alla salute delle persone che abbiano scaricato liberamente la app e quindi siano entrate "liberamente" a far parte di questo sistema di tracciamento è particolarmente interessante e meritevole di attenzione.
Questo richiamo e questo vincolo imposto al punto 31 delle Linee guida 04/2020, adottate il 21 aprile 2020, soprattutto in quanto accompagnato dal vincolo a che l'inserimento nel sistema dei dati sanitari richieda comunque l'intervento di un operatore sanitario tenuto al segreto professionale (cfr. anche punto 36 delle Linee guida citate), dimostrano con chiarezza che lo EDPB non ha voluto solo esprimere un parere favorevole rispetto alla app denominata Immuni, che infatti non viene presa in considerazione espressamente.
In sostanza, infatti, con queste Linee guida lo EDPB ha voluto dettare, in via generale, criteri interpretativi delle norme del GDPR, incidendo in tal modo anche sulla loro applicazione e, quindi, rendendo di fatto potenzialmente residuale l'intervento esplicito del decisore UE o di quello statale previsto dall'art. 9 del GDPR.
In realtà, tuttavia, le Linee guida dello EDPB sono ancora più sofisticate. Esse, infatti, si incardinano con evidente chiarezza in quanto previsto al punto 31, laddove si chia-

risce che le app che consentono tracciamenti, anche per le ragioni previste dall'art. 9, sono compatibili con il GDPR solo a condizione che non ne sia reso obbligatorio l'uso. Proprio nell'obbligo di prevederne la totale libertà di scaricamento sul device telefonico si incentra il contenuto essenziale di queste Linee guida, come dimostra il fatto che, in base al punto 32, il consenso diventa una base puramente "eventuale" di legittimità del trattamento. Resta fermo, tuttavia, che se la legittimazione dei trattamenti si basa essenzialmente sul consenso da parte dell'interessato questo implica poi che siano soddisfatti i requisiti collegati a tale base giuridica, primo fra tutti la revocabilità in qualunque momento del consenso stesso.

In sostanza, par di capire, il ragionamento che sottostà alle Linee guida adottate dallo EDPB è che secondo questo organo l'art. 9 fonda proprio sul consenso, considerato come la prima base giuridica che legittima il trattamento di dati personali relativi alla persona che tale consenso esprime, la tutela della sovranità degli interessati rispetto ai loro dati personali e, dunque, il rispetto della tutela dei loro dati come fondamento della libertà, e condizione essenziale per la tutela di tutti i diritti fondamentali previsti dalla UE.

È una evidente conferma di questo il fatto che se il consenso non è richiesto o previsto, allora lo scaricamento della app deve essere libero e non può in alcun modo essere imposto dalla legge.

In sostanza lo EDPB sembra aver ragionato nel senso che è possibile consentire l'uso di una app di tracciamento anche senza richiedere l'esplicito consenso dell'interessato solo a condizione che il suo scaricamento sia libero e mai imposto obbligatoriamente per legge (né, sembra doversi dedurre, per obbligo imposto da altri).

È chiaro che, in questo modo, il mancato consenso esplicito, che per altro comporta anche la revocabilità del consenso stesso, può essere pretermesso perché l'interessato è totalmente libero di decidere se scaricare o no la app e di conseguenza rendere possibili i tracciamenti e l'utilizzazione a tal fine della app scaricata (sempre ovviamente che la persona sia stata adeguatamente informata delle modalità di funzionamento della app e delle tutele relative ai trattamenti che saranno posti in essere, ivi compresa l'avvenuta elaborazione di una adeguata DPIA).

A queste condizioni, infatti, lo scarico dell'applicazione, purché accompagnato da una informativa coerente con i criteri di cui agli artt. 13 e 14, e con quanto stabilito dalla Linee guida in questione, può tenere il posto del consenso, il che evita di dover predisporre le modalità da seguire per esercitare il diritto alla revoca di un consenso che, altrimenti, dovrebbe essere sempre revocabile.

Tutto questo è confermato dal punto 32 che, infatti, ricorda coerentemente che se però una app di tracciamento si basa sul consenso, e dunque rispetta esplicitamente il primo dei criteri indicati dall'art. 9 del GDPR, allora è necessario che il sistema assicuri anche la soddisfazione di tutti i requisiti collegati a tale base giuridica, primo fra tutti la revocabilità del consenso stesso.

L'aspetto fondamentale delle Linee guida dello EDPB, presente già anche nelle lettere della sua Presidente Andrea Jelinek, sta dunque nell'aver di fatto sostituito il principio del consenso, quale presidio "principe" della libertà della persona legata all'uso dei dati che la riguardano, col diverso principio della libera scelta e decisione relative all'uso di

app o altri sistemi tecnologici che consentano di utilizzare, anche senza esplicito consenso, i dati personali per tracciare la persona alla quale essi si riferiscono.
Per contro, ovviamente, la possibilità per le Autorità garanti di adottare (o meglio imporre) misure di garanzia e tutela dei dati personali in un quadro derogatorio rispetto al GDPR è molto limitata. Lo dimostrano anche le Linee guida richiamate che, infatti, sostanzialmente richiamano, anche a titolo di rafforzarne l'effetto, obblighi già previsti dal GDPR, quali ad esempio, il dover procedere a una accurata DPIA circa i trattamenti posti in essere dalle app scaricabili, senza però aggiungere, né poter aggi ungere, nuovi obblighi specifici, eventualmente ragionevolmente connessi alla specificità dei rischi che l'uso della app può comportare. Il punto è interessante perché proprio i primi giorni di uso della app Immuni hanno fatto rilevare casi di allarmi inviati a specifici interessati senza che i dati a disposizione del sistema lo richiedessero e giustificassero, come espone anche l'avv. Lisi nell'articolo "*E se Immuni impazzisse? I primi segnali ci sono e finiremmo tutti prigionieri*", in *Il Fatto quotidiano* del 26 giugno 2020.
Da questo punto di vista le Linee guida dello EDPB sono estremamente istruttive perché, sulla stessa scia del divieto di rendere obbligatoria la installazione della app, richiamano, in termini di raccomandazioni o di vincoli, elementi già contenuti nello stesso art. 9 o comunque strettamente legati alla logica del GDPR, come ad esempio il principio di minimizzazione, di finalità, di valutazione di impatto e anche di interoperabilità delle app a livello UE. In particolare, quest'ultimo principio legato alla interoperabilità è indicato come strettamente legato al principio di finalità legata alla lotta all'epidemia. Tuttavia, la raccomandazione relativa alla interoperabilità a livello UE è fondata anche sulla necessità di assicurare un «clima di fiducia» necessario a «creare le condizioni per l'accessibilità sociale di qualunque soluzione e garantire pertanto l'efficacia di tali misure» (cfr. punto 3 delle Linee guida). Proprio quest'ultimo punto è particolarmente importante perché testimonia che lo EDPB è molto attento a richiedere sempre anche il pieno rispetto del principio di accountability relativo alle soluzioni proposte, nella consapevolezza che solo una applicazione "*accountable*" rispetto alle finalità perseguite è compatibile col GDPR, Solo a queste condizioni, infatti, tale applicazione può soddisfare anche le condizioni di affidabilità necessarie a ottenere la fiducia degli interessati rispetto ai trattamenti dei loro dati. Uno dei punti, questo, più importanti del sistema regolatorio relativo ai trattamenti dei dati personali così come disegnato dal GDPR

6. In sostanza almeno quattro sono gli aspetti essenziali che caratterizzano le Linee guida dello EDPB, tutti meritevoli di essere sottolineati con forza.
La messa al centro di tutto il ragionamento svolto del principio di "responsabilizzazione" che, anche nel significato terminologico della espressione, ha un significato diverso dal consenso. Ed è proprio grazie al fatto che implicitamente si sostituisce il consenso col principio di responsabilizzazione che si può considerare equipollente a un consenso non richiesto la decisione di scaricare la app, purché ovviamente questa decisione non sia obbligata o imposta dalla legge, né, sembra di poter dire, da alcun altro soggetto.
È evidente tuttavia che la sostituzione del concetto di consenso con quella di responsabilizzazione comporta anche una riflessione sul ruolo della informativa che deve essere

data. Se questa informativa deve essere finalizzata al rendere effettivo il principio di responsabilizzazione deve consentire una scelta "responsabile", e dunque basata sulla piena consapevolezza non solo del funzionamento della app ma anche delle sue finalità e delle conseguenze che il tracciamento può comportare sia per le persone che la hanno scaricata che per quelle i cui dati personali sono trattati dalla app stessa.
Inoltre, deve essere chiaro che se il principio di responsabilizzazione è soddisfatto solo grazie alla decisione non vincolata dell'interessato di scaricare la app sul proprio device, allora solo l'interessato può decidere responsabilmente sull'uso dei propri dati. Tutti gli altri, i cui devices entreranno eventualmente in contatto nel tempo, consentendo quindi trattamenti dei loro dati personali grazie a questa app non possono incidere in alcun modo sui trattamenti che ne seguiranno. È qui che, come si vedrà più avanti, torna ad essere essenziale il ruolo della informativa adeguata, giacché solo una informativa chiara e pienamente esaustiva sul funzionamento della applicazione può consentire a tutti gli interessati aderenti al sistema di conoscere sia i trattamenti dei loro dati già possibili al momento della decisione di scaricare la app che quelli che potranno essere effettuati nel tempo, mano a mano che la rete dei soggetti coinvolti per loro libera scelta nell'uso dell'applicazione, decideranno a loro volta di scaricarla.
Dunque, il principio di responsabilizzazione, come è ovvio, riguarda non solo e tanto i trattamenti che in concreto potranno essere posti in essere a seguito dello scarico della app quanto, e soprattutto, la tecnologia utilizzata e le conseguenze che essa può comportare in termini di trattamento dei dati in futuro.
In sostanza la decisione relativa a consentire i trattamenti dei propri dati è qualitativamente e giuridicamente diversa da quella relativa all'accettare o meno di servirsi di una specifica tecnologia scaricando la app relativa.
È ragionevole dire che le Linee guida avrebbero dovuto essere più chiare ed esplicite di quanto siano anche rispetto a questo specifico punto, relativamente, cioè, alla informativa da dare prima che la app sia scaricata.
Questo profilo è tanto più importante giacché, come le Linee guida sottolineano più volte, al caso in esame si applica non solo il GDPR e, in particolare, l'art. 9, ma anche la Direttiva e-Privacy 2002/58/CE e in particolare l'art. 5, che prevede anche deroghe ulteriori rispetto alle norme di tutela dei dati personali che siano collegate a trattamenti nell'ambito delle comunicazioni elettroniche.
È proprio in virtù dell'art. 5 della direttiva 2002/58/CE che lo EDPB precisa che comunque il consenso deve restare un principio rispettato come fondamentale per quanto riguarda l'uso dei dati raccolti attraverso la app liberamente scaricata per i fini previsti dall'art. 23 del GDPR.
Dunque, il principio del consenso, uscito dalla porta per far spazio al principio di responsabilità, rientra attraverso l'art. 5 della direttiva 2002/58, a dimostrazione di quanto rilevanti siano le conseguenze relative al mancato aggiornamento di questa direttiva. Aggiornamento che, nei piani della Commissione, avrebbe dovuto avvenire contestualmente alla entrata in vigore del GDPR.
Inoltre, il richiamo all'art. 5 della direttiva mostra anche i limiti della prospettiva seguita dallo EDPB nel formulare queste Linee guida.
Le Linee guida richiamano tutto questo al punto 13, ma poi non approfondiscono

adeguatamente su come tale consenso dovrebbe specificamente essere comunicato e raccolto, e da chi a chi, e quando e come.
Le Linee guida, infatti, soprattutto con riguardo ai dati relativi all'ubicazione degli interessati, preferiscono accentuare il principio della anonimizzazione dei dati e le modalità della applicazione.
Temi, questi, che occupano di fatto tutti i punti da 14 a 23 delle Linee guida e che, se correttamente applicati, consentono di superare il principio del consenso rispetto ai singoli trattamenti proprio perché i dati anonimizzati non sono considerati sottoposti ai limiti di trattamento previsti dal GDPR.
Ne consegue, dunque, che mentre da un lato si afferma di voler sottolineare il principio di responsabilizzazione in luogo di quello del consenso, dall'altro, in ultima analisi, si nega l'applicazione del principio del consenso non solo in virtù degli effetti di responsabilizzazione delle modalità tecnologiche adottate seguendo le indicazione dello EDPB ma anche perché esse consentono la anonimizzazione dei dati oggetto di raccolta e di trattamento e, dunque, permettono di escludere dalla applicazione della normativa di protezione dei dati personali i trattamenti relativi alle modalità di funzionamento dell' applicazione.
Ovviamente, così facendo lo EDPB sposta nuovamente il focus delle Linee guida dagli aspetti giuridici a quelli tecnologici e ciò non può non richiedere e imporre una informativa specifica verso gli interessati. Informativa che, ovviamente, deve essere fornita prima che la app sia scaricata perché riguarda proprio la decisione di scaricare o no la app e dunque l'aspetto essenziale dell'attuazione del concetto di "responsabilizzazione" così come impostato dallo EDPB.
Infine, con riguardo al principio di finalità, elemento essenziale per valutare sia la legittimità della raccolta dei dati che quella dei loro trattamenti, lo EDPB ribadisce che la finalità è legata alla lotta all'epidemia Covid-19. Il che significa che i trattamenti in tanto sono legittimi in quanto i dati trattati, sia con riferimento alla loro raccolta che alla loro utilizzazione, devono essere coerenti col perseguimento di tale fine che, come si è detto, secondo lo EDPB richiede la interoperabilità tra i sistemi adottati nei diversi Paesi e la messa in campo di trattamenti a tale scopo finalizzati almeno con riferimento al territorio degli Stati membri della UE (cfr. punto 6 della Linee guida).
Anche di questo, se il quadro deve essere quello della responsabilizzazione della persona e del rafforzamento della sua assunzione di responsabilità, va data adeguata informativa prima che la app sia scaricata, indicando anche, sembra naturale ritenere, quali siano le app utilizzate negli altri Paesi, come i dati raccolti da ciascuna di esse possano essere utilizzati da tutte e con quali tecnologie di protezione e tutela delle informazioni.
Purtroppo anche di questi aspetti nelle Linee guida dello EDPB non vi è praticamente traccia, mentre è qui che avrebbe potuto trovare spazio una soddisfacente analisi degli effetti dell'uso, da parte della app Immuni della piattaforma tecnologica comune di Google e di Apple, anche superando i problemi, tutt'altro che irrilevanti, legati al trasferimento dei dati all'estero e la scarsa garanzia di tutela rispetto ai trattamenti di tali dati potenzialmente svolti dai due soggetti titolari della piattaforma comune.

7. Infine, merita tenere presente che non è chiaro chi sia il destinatario delle Linee

guida.
Infatti, mentre il destinatario della lettera della Presidente Jelinek del 14 aprile 2020 è direttamente la Commissione nella persona del dr. Micol, a una specifica richiesta del quale la lettera stessa intende rispondere, le Linee guida del 21 aprile sono una autonoma iniziativa dello EDPB anche se, ovviamente, finalizzata a fornire indicazioni relative al fatto che, come si dice al punto 1, «Governi e soggetti privati si stanno orientando verso l'uso di soluzioni basate sui dati nell'ambito della risposta alla pandemia causata dal Covid-19, e ciò suscita numerose preoccupazioni in materia di tutela della vita privata».
Dunque, le Linee guida sono una autonoma iniziativa dello EDPB, i cui destinatari sembrano essere non tanto i legislatori o i decisori UE o statali, quanto direttamente le Autorità garanti di protezione dei dati personali. Solo a questi, infatti, possono essere rivolte indicazioni che fissano paletti relativamente all'uso, *compliant* con il GDPR, di app finalizzate al tracciamento delle persone.
Va detto inoltre che nelle Linee guida dello EDPB lo stesso riferimento alla situazione di epidemia come causa giustificativa dell'uso di app di tracciamento è assai poco richiamato. Soprattutto è assai poco sottolineata la connessione tra l'uso delle app di tracciamento dei dati e le eventuali esigenze di sanità pubblica, richiamate invece con forza dall'art. 9, par. 2, lett. *i*).
Infatti, il punto 4 delle Linee guida, a giustificazione dell'adozione delle app di tracciamento, non si riferisce tanto la lotta alla epidemia e ai motivi di interesse sanitario quanto piuttosto al fatto di «dare maggiori strumenti alle persone, piuttosto che stigmatizzarle o reprimerne i comportamenti».
Inoltre, aggiunge lo EDPB, «mentre i dati e le tecnologie possono essere strumenti importanti, essi hanno limiti intrinseci e non possono far leva sull'efficacia di altre misure di sanità pubblica». Il che significa che la compatibilità tra i tracciamenti dei dati relativi alle persone e le regole di protezione dei dati personali deve basarsi sul rispetto dei «principi di efficacia, necessità e proporzionalità da valutare rispetto a qualsiasi misura adottata dagli Stati membri o dalle istituzioni della UE che comporti il trattamento di dati personali per combattere il COVID-19» (cfr. punto 4 delle Linee guida).
Le Linee guida sembrano dunque collocarsi in una prospettiva molto diversa dall'art. 9 del GDPR non solo perché sostituiscono il principio di responsabilità al principio del consenso ma anche perché rovesciano completamente il rapporto tra ruolo di tecnologie di tracciamento e misure sanitarie decise dalla UE o dagli Stati membri. Non sono infatti le misure sanitarie e l'efficacia delle tecnologie adottate a raggiungere l'obiettivo i parametri sui quali valutare gli effetti delle app rispetto alla loro compatibilità con la normativa di tutela dei dati personali (come sembra essere nell'art. 9, par. 2, lett. *i*). Quello che, secondo queste Linee guida, deve guidare nella valutazione della compatibilità tre le app e il GDPR della app è il rispetto in sé dei principi di efficacia, necessità e proporzionalità, come indicatori delle finalità di tutela della libertà degli interessati, che la app deve concorrer a garantire attraverso i trattamenti dei dati da loro consentiti. Questa sembra, infatti, la ragione per la quale le Linee guida specificano che le app adottate e i dati raccolti e trattati «devono guidare qualsiasi misura adottata dagli Stati membri o dalle istituzione della UE che comporti il trattamento di dati personali per

combattere il COVID-19». Ed è in questa prospettiva che si comprende perché si precisi che il rispetto di questi principi deve essere verificato per stabilire la compatibilità delle misure adottate con il GDPR.
Insomma, a una prima lettura le Linee guida dello EDPB del 21 aprile 2020 sono un documento il cui scopo principale pare essere quello di superare il principio del consenso sostituendolo con quello di responsabilità, declinato essenzialmente con attenzione alle modalità tecnologiche legate all'utilizzazione delle app di *tracing* e, ma molto meno, con riguardo al contenuto specifico delle informative da fornire.
A una lettura più attenta, tuttavia, il vero effetto delle Linee guida è di fatto quello di sganciare il collegamento tra la adozione delle app e il loro essere *compliant* con il GDPR dal ricorrere delle circostanze di cui al par. 2, lett. *i*), dell'art. 9 del GDPR, e dunque da una specifica valutazione dei decisori unionale e nazionali sulla necessità dei tracciamenti per «motivi di interesse pubblico nel settore della sanità pubblica» (come invece afferma l'art. 9, par. 2, lett. *i*). Il collegamento sul quale si fonda la compatibilità col GDPR si basa unicamente, o essenzialmente, sul fatto di «dare maggiori strumenti alle persone», nel rispetto dei principi fondamentali della protezione dei dati personali, che vengono puntualmente richiamati al punto 4 delle Linee guida.
I punti più deboli, almeno a mio parere, sono tuttavia quelli legati alla mancanza di indicazioni chiare ed esaurienti circa le informative da fornire e il loro contenuto. Aspetti, questi, essenziali anche e soprattutto nel quadro del principio di responsabilizzazione e di quello relativo alla affermata necessità di rispetto della direttiva relativa alla vita privata e alle comunicazioni elettroniche, soprattutto con riguardo all'art. 5 e alla necessità di dare e avere specifici consensi relativi ai diversi trattamenti.
Si potrebbero richiamare anche altri aspetti, già accennati nel corso di questa analisi, ma è possibile fermarsi qui, non senza richiamare il fatto che le Linee guida ribadiscono il principio di finalità, estendendolo addirittura a un uso su scala continentale della tecnologia di tracciamento, senza poi individuare alcuna concreta modalità da adottare al fine di accertare che tale condizione sia rispettata e senza specificare a chi spetti compiere tale verifica.
È evidente, dunque, che le Linee guida in esame, mentre da un lato dimostrano concretamente l'importanza delle norme relative alla protezione dei dati personali anche di fronte all'utilizzazione, ai fini di trattamenti specifici, di nuove tecnologie che possono esaltare il principio di responsabilizzazione dell'interessato, dimostrano contemporaneamente quanto fondata sia l'esigenza di porre particolare attenzione a una "rilettura" delle stesse norme europee e delle loro modalità di applicazione, al fine di verificare la compatibilità delle nuove tecnologie con un sistema regolatorio certamente in forte tensione fin dal momento della sua entrata in vigore rispetto all'evoluzione di una realtà digitale in continuo mutamento e sviluppo.

8. Peraltro, come si è sottolineato più volte nel corso di questa analisi, il GDPR è stato, fin dall'inizio, perfettamente consapevole della possibilità che le tecnologie, soprattutto se usate per finalità di particolare rilievo, quali quelle ben indicate nell'art. 9 secondo capoverso, potessero implicare o richiedere il superamento di specifiche norme in esso contenute, o almeno applicazioni delle norme coerenti con le caratteristiche tecnologi-

che dei trattamenti di volta in volta previsti o disponibili.
Del resto, dello stesso fenomeno era già stata consapevole la direttiva relativa alle comunicazioni elettroniche e la vita privata del 2002. Ancora di più: proprio l'elasticità e adattabilità all'evoluzione delle tipologie di trattamenti strettamente connesse a tutta l'architettura del GDPR non è che la manifestazione "sistemica" della consapevolezza che l'evoluzione tecnologia è destinata inevitabilmente a richiedere letture innovative delle disposizioni del GDPR, e comunque applicazioni attente a rispettare più la sostanza del contesto normativo che la lettera delle singole disposizioni, specialmente dove una lettura prevalentemente burocratica diventasse impeditiva del raggiungimento di finalità che lo stesso GDPR mostra di apprezzare.
Il punto essenziale è che entrambe le richiamate normative UE, e soprattutto l'art. 9 del GDPR, rimettevano e rimettono ai decisori UE e nazionali la valutazione circa il "giusto punto di equilibrio" tra diritti fondamentali tra loro in tensione e la decisione su come assicurare che la compressione delle norme europee non avvenga pregiudicando ogni tutela e garanzia della protezione dei dati personali.
Nelle Linee guida in esame, invece, lo EDPB, sostituendo al principio del consenso quello della responsabilizzazione come via maestra per tutelare la libertà delle persone, individua una strada che consente allo EDPB stesso e poi alle singole Autorità garanti, senza necessità di intervento dei decisori UE e nazionali, di operare tale bilanciamento e verificarne, anche sotto i profili tecnologici, il rispetto.
Operazioni, queste ultime, che le Linee guida fanno sia rispetto all'art. 9 del GDPR, sostituendo il principio di consenso col principio di responsabilizzazione; sia affermando che la tecnologia può consentire di conciliare il raggiungimento delle finalità perseguite anche con la anonimizzazione dei dati, escludendo in tal modo la applicabilità delle regole di protezione dati sia del GDPR che della direttiva del 2002 sulla vita privata e le comunicazioni elettroniche.
Inoltre, con le Linee guida in esame lo EDPB fissa anche specifici principii e criteri che le tecnologie adottate devono garantire, soprattutto con riguardo al rispetto del principio di finalità dei trattamenti. In tal modo si rende superfluo, anche su questo piano, l'intervento del decisore UE e di quelli nazionali.

9. In questo quadro, che poggia largamente da un lato su una rilettura, spesso "compiacente" ma non per questo "inappropriata", della normativa UE, e dall'altro su una "analisi aperta e costruttiva" delle potenzialità delle tecnologie adottate, lo EDPB (e soprattutto le Autorità garanti nazionali) diventano anche, sia pure nell'ambito della compatibilità tra dettato normativo e innovazione tecnologica, i tutori di fatto della libertà delle persone legata alla tutela dei loro dati personali. Una tutela che, nel quadro delle Linee guida, appare molto più fondata sui limiti e i vincoli posti alle tecnologie usate e al loro rapporto coi principi di responsabilità e di finalità che non sulla difesa del principio del consenso come strumento essenziale di libertà, in virtù del quale nessuno può usare i dati di una persona se non per finalità stabilite dalla legge, o per tutelare i diritti fondamentali stessi dell'interessato, o senza il consenso adeguatamente informato di questi, salvo che si tratti di casi in cui i trattamenti sono esplicitamente consentiti dal legislatore cui spetta anche fornire altre e adeguate garanzie e tutele.

È pacifico dunque che le Linee guida in questione, se ben lette e contestualizzate dentro il quadro complessivo della tutela dei dati personali, costituiscono un salto di qualità molto importante, sia rispetto al ruolo delle Autorità garanti (e in particolare dello EDPB), sia rispetto al ruolo della normativa di protezione dei dati personali.

10. Rispetto al ruolo della Autorità garanti il salto di qualità operato dalle Linee guida è del tutto evidente.
Mentre il GDPR definisce in termini molti ristretti e, soprattutto, molto specifici, l'ambito regolatorio proprio delle Autorità, la prospettiva aperta dalle Linee guida appare fare dello EDPB una sorta di Corte costituzionale settorialmente competente in materia di tutela dei dati personali. Allo stesso tempo fa implicitamente delle Autorità nazionali il tramite attraverso il quale assicurare che le decisioni e le indicazioni dello EDPB siano concretamente rispettate, anche al fine di aumentare la fiducia dei cittadini nella tutela delle loro libertà. Senonché proprio il ruolo della Autorità garanti resta troppo implicitamente definito e potenzialmente anche non sufficientemente omogeneo.
Di fatto, proprio perché le Linee guida si limitano a indicare i vincoli essenziali a tutela dei cittadini che le attività di tracciamento devono rispettare rimettendo poi prima agli operatori e infine ai Garanti nazionali il compito di garantire che tali indicazioni siano rispettate, si potrebbe verificare facilmente una sorta di "geopardizzazione" della tutela dei dati personali a seconda del modo col quale le Autorità garanti esercitassero in concreto i propri impliciti poteri di vigilanza. È vero che la medesima cosa potrebbe accadere anche se si desse piena attuazione all'art. 9 attraverso regolazioni nazionali dei principi richiamati in quella norma, ma è vero anche che in questo caso il controllo sul decisore UE e sui decisori nazionali potrebbe essere facilmente esercitato dalla Corte di giustizia o dalle Corti nazionali, a seconda dei casi, e comunque i cittadini avrebbero la loro tutela legata direttamente all'intervento dell'autorità giudiziaria anche ai fini di controllo della compatibilità tra legislazione nazionale e normativa UE. Controllo, questo, certamente più "robusto" di quello di fatto rimesso alle Autorità garanti, anche perché le Corti possono adottare criteri più generali e meno legati ai singoli casi concreti di quanto possano fare invece le Autorità, il cui intervento è sempre legato ai singoli casi. Inoltre, non va dimenticato che, comunque, in questa ipotesi oggetto del controllo del giudice sarebbe la compatibilità col GDPR di regole adottate in forma di legge o con fonte assimilabile, e non valutazioni relative alle verifiche poste in essere rispetto alla adozione di tecnologie specifiche e alle relative tutele adottate.

11. Questo effetto delle Linee guida adottate dallo EDPB in occasione delle app di tracciamento nel contesto della epidemia di Covid-19 è particolarmente rilevante proprio perché, come si è detto al paragrafo precedente, le Linee già hanno ad oggetto il rapporto tra l'utilizzazione di app di tracciamento dei comportamenti delle persone in via generale e non specificamente nell'ambito della lotta all'epidemia di Covid-19.
Proprio questo aspetto, del resto, rende particolarmente importanti le riflessioni qui svolte. Infatti, la conseguenza delle scelte operate con le Linee guida 04/2020 va ben oltre il quadro legato alla lotta all'epidemia. Di fatto esse sembrano orientate a definire la base sulla quale fondare i vincoli di ogni app di tracciamento delle persone, quali che

siano le finalità di volta in volta perseguite.

12. Proprio queste ultime riflessioni giustificano che si chieda sia allo EDPB che ai Garanti nazionali maggiore cautela nel sostituirsi ai legislatori o, se si preferisce, ai decisori, soprattutto quando è la stessa normativa di protezione dei dati personali che rimette a questi ultimi il compito di garantire adeguate tutele agli interessati.
Su questo punto merita essere chiari. Per un verso la linea seguita dallo EDPB con la adozione delle Linee guida 04/2020 è assolutamente apprezzabile perché apre la strada a una ulteriore, e necessaria, flessibilità del GDPR, che in futuro potrà estendersi anche ad altre applicazioni tecnologiche, come ad esempio la blockchain e l'utilizzazione di forme più strutturate di bitcoin o di pagamenti in modalità telematica, anche ampliando l'uso della *privacy by design* o *by default*. Principi, questi ultimi, di carattere tecnologico di grande potenzialità, che il GDPR prevede ma che non hanno ancora trovato pieno sviluppo nel corso del biennio dalla sua entrata in vigore.
Inoltre, è assolutamente condivisibile e apprezzabile lo sforzo esplicito fatto dallo EDPB di sostituire, quasi senza dare a ciò troppa importanza, il principio di tutela della responsabilità della persona rispetto al principio del consenso come garanzia basica della possibilità di autotutela da parte degli interessati rispetto ai loro dati.
Non vi è dubbio, infatti, che il principio del "consenso", certamente molto efficace nella fase iniziale della normativa di protezione dei dati personali anche per il suo significato sostanziale, che ha sempre consentito di sottolineare che, almeno in via generale e salvo le eccezioni legislativamente specificate, nessuno può trattare dati di un altro senza il suo consenso, proprio perché i dati personali sono della persona alla quale si riferiscono, è venuto via via mostrando tutti i suoi limiti, soprattutto dal punto di vista della inevitabile connessione col principio secondo il quale laddove il consenso è necessario questo deve poter essere sempre revocabile.
È ovvio che, in un contesto nel quale le tecnologie evolvono continuamente, la possibilità di revocare in qualunque momento il consenso già dato al trattamento di propri dati personali può determinare conseguenze negative nei confronti di un numero indefinito di interessati, come certamente avverrebbe nel caso di immuni, soprattutto laddove il sistema nel suo complesso riuscisse davvero, una volta a regime, a garantire una forte tutela nei confronti di tutti coloro che avessero deciso di aderire ad esso scaricando di conseguenza la app Immuni.
Va detto che, anche per questo, appare anche particolarmente "sottile" e "interessante" la scelta di puntare tutto sul principio di responsabilità piuttosto che sul consenso, imponendo a tal fine che la scelta di scaricare o meno la app sia riservata gelosamente e unicamente ai potenziali interessati. Una scelta che in questo caso è resa possibile dalla necessità di scaricare la app, che non è preinstallata sui devices. Si tratta tuttavia di una linea che appare difficilmente conciliabile col fatto, che le Linee guida sottolineano, secondo il quale perché il sistema sia efficace è fondamentale che un ampio numero di interessati abbiano scaricato sui loro devices la app (cfr. Linee guida, n. 6).
Appare dunque particolarmente "forte" il collegamento fatto dalle Linee guida tra la assoluta volontarietà dell'installazione della app di tracciamento sul proprio telefonino e il principio di responsabilità. Il collegamento, per la verità non troppo esplicito, tra

questi due aspetti è molto rilevante anche in prospettiva, tanto più perché è applicato anche in un contesto nel quale, perché il sistema raggiunga in modo affidabile le sue finalità e i suoi scopi, è necessario che la app sia scaricata da una percentuale molto elevata di cittadini: cosa quest'ultima che avrebbe caso mai potuto spingere a chiedersi se, perché tutto il sistema sia davvero efficace e raggiunga i propri scopi, non si sarebbe caso mai dovuto ragionare in modo opposto, superando il principi del consenso in favore della obbligatorietà piuttosto che della piena e autonoma libertà di scaricamento. Anche per questo è evidente l'attenzione che lo EDPB ha riservato alla gelosa tutela della salvaguardia della libertà e della autonomia delle persone. Ed è proprio da questo punto di vita che le Linee guida in esame possono avere specifico rilievo anche in futuro, rispetto a ulteriori e diverse utilizzazioni di altre innovazioni tecnologiche, ivi comprese ovviamente nuove e divere app di tracciamento per finalità diverse da quelle del caso in esame.
È evidente, insomma, che lo EDPB ha ritenuto opportuno cogliere questa occasione non solo per indicare i vincoli che il ricorso al tracciamento di dati personali tramite app deve rispettare, ma anche per riaffermare la necessità di una interpretazione e applicazione "flessibile" delle norme di protezione dati, irrobustendo nell'occasione la più rigorosa tutela della libertà della persona e del principio di responsabilità, assicurato in questo caso grazie alla libertà di scelta dell'interessato di avvalersi o meno della app.
È chiaro inoltre che queste Linee guida, che pure rimettono a ciascuna app il compito di adeguarsi alle indicazioni date, adottando DPIA efficaci a valutare i rischi e ad assicurando misure conseguenti, anche con riguardo ai punti specifici analizzati dalle Linee guida stesse (cfr. soprattutto la parte 3.2. delle Linee guida), aprono la via a una evoluzione futura molto importante del ruolo dei poteri dello EDPB e elle Autorità garanti nazionali.

13. In sostanza, la decisione di sostituire con indicazioni date dallo EDPB e dai Garanti nazionali, ai quali spetta poi verificarne anche il rispetto, le indicazioni che invece, sia *ex* art. 9 che art. 23 del GDPR sarebbero spettate caso mai al decisore unionale o a quelli statali, costituisce un salto in avanti molto forte rispetto alla lettura finora data della flessibilità del GDPR e del ruolo delle Autorità di Garanzia.
Di fatto queste Linee guida trasformano la flessibilità propria del GDPR nel fondamento di una attività multifunzionale delle Autorità garanti. Ne deriva una espansione molto forte del ruolo delle Autorità e dei poteri consultivi loro riconosciuti, che è già in parte adombrata in numerose norme del GDPR ma che trova ora in queste Linee guida le premesse, anche teoriche, di un suo rapido sviluppo.
Di tutto questo ci accorgeremo rapidamente e probabilmente in modo particolare proprio con riguardo alle app di tracciamento che sono certamente destinate a moltiplicarsi e il cui uso potrà interessare molti settori diversi, anche lontani dal settore sanitario e, ancor più, dal fenomeno epidemico.
A questo si deve aggiungere fin da ora la prevedibilissima espansione delle premesse già indicate in queste Linee guida, che potranno essere utilizzate per ampliare il ruolo delle Autorità garanti e delle loro Linee guida anche a nuove, già oggi prevedibili e in atto, innovazioni tecnologiche, a partire proprio dalla precisazione di come attuare i

principi di *privacy by design* e *by default* nei settori di maggior sviluppo tecnologico nei prossimi anni.
Né è difficile pensate che sulla strada aperta dalle Linee guida in commento le Autorità garanti saranno tentate (e forse anche richieste) di dare indicazioni importanti sia sull'uso delle applicazioni basate sull'Intelligenza Artificiale che di quelle funzionali a una espansione ampia, e già in pieno sviluppo in mezzo a noi, della robotica "intelligente", che può andare dalle macchine a guida autonoma fino ai robot antropomorfi.

14. Tutte le considerazioni svolte spingono dunque a richiamare con forza l'attenzione sulle Linee guida 04/2020 dello EDPB, non solo e non tanto per gli aspetti relativi alla app Immuni o alle app di tracciamento quanto, e soprattutto, per il rilevante mutamento che esse comportano sia rispetto al ruolo dei Garanti che alle modalità di evoluzione della normativa di protezione dei dati personali e delle sue applicazioni rispetto alla prevedibilissima e inevitabile crescita della società digitale e delle sue applicazioni future.
Né è possibile affermare che questo fenomeno sia censurabile giacché è sempre più evidente che lo sviluppo del mondo digitale e dei trattamenti dei dati ha subito una enorme accelerazione con il verificarsi dell'epidemia, aprendo così la strada al passaggio del mondo e degli esseri umani che lo abitano a una fase del tutto nuova, nella quale è chiara la centralità dei dati e delle loro modalità di analisi, da un lato, la continua difficoltà di individuare il punto di equilibrio corretto tra la tutela del diritto fondamentale alla tutela dei dati, specialmente personali, che nella società digitale è l'architrave di ogni libertà, con la tutela non solo degli altri interessi e diritti fondamentali individuali (da quello alla salute a quello della difesa della vita stessa) ma anche dei diritti fondamentali collettivi, che spesso possono trovare nel trattamento di quantità sempre crescenti di dati la condizione per la loro piena espansione e per l'ottimizzazione dell'uso delle nuove tecnologie per la sicurezza e la tutela dei valori fondamentali sia degli individui che delle collettività sociali alle quali essi appartengono.
Di qui non solo l'enorme accelerazione che lo sviluppo della società digitale avrà nei prossimi anni ma anche il manifestarsi sempre più evidente che a una nuova fase della storia del mondo deve accompagnarsi un profondo ripensamento delle sue regole giuridiche e un forte rafforzamento delle tutele essenziali per le libertà fondamentali degli esseri umani.
In pericolo c'è certamente la libertà individuale ma c'è anche, e molto e molto di più, la natura ontologica stessa della libertà degli esseri umani, almeno così come la percepisce la cultura, la filosofia e la scienza di matrice occidentale.
Tutto questo consente di dire che non solo sarà molto importante seguire con attenzione come i principi e le regole contenuti in queste Linee guida saranno sviluppati e troveranno attuazione rispetto alle app di tracciamento (a partire ovviamente da Immuni). Sarà anche molto importante osservare se e come le Autorità garanti e lo EDPB intenderanno nel prossimo futuro sviluppare i principi che sottostanno a queste Linee guida, anche allo scopo di aprire una nuova stagione nella quale le Autorità devono essere impegnate anche a garantire non solo una adeguata flessibilità della protezione dei dati personali di fronte allo sviluppo delle tecnologie, ma anche e soprattutto un

crescente, importante e prezioso ampliamento del loro ruolo di Autorità garanti.
Autorità che nel nuovo mondo digitale dovranno sempre meno essere guidate da una visione burocratica di controllo sull' applicazione delle norme per privilegiare invece sempre di più una tutela dinamica della salvaguardia dei loro contenuti e dei valori che vi sottostanno. Una attività capace di sviluppare e adeguare i principi fondamentali della tutela di questo diritto (essenziale per la libertà di tutti e di ciascuno) alla nuova fase della storia nella quale, anche come effetto del Coronavirus, ormai tutto il mondo è coinvolto.
Non vi è dubbio che tutto questo è perfettamente coerente allo spirito e all'ampiezza di visione del GDPR, che non a caso ha così fortemente rafforzato i poteri regolatori delle Autorità e il ruolo dello EDPB come garante dell'omogeneità dello sviluppo delle attività proprie dei Garanti. Non vi è nemmeno dubbio, tuttavia, che tutto questo comporta che anche le Autorità e i cultori della protezione dei dati personali sappiano rapidamente sviluppare forme nuove e proattive di approccio ai temi che sono e saranno chiamati ad affrontare.
Il tempo futuro non può essere quello dominato da un diritto minuziosamente prescrittivo e da norme descrittive e regolatrici di ogni profilo possibile dei beni e dei valori fondamentali che intendono proteggere. Il mondo nuovo, e tanto più la sua dimensione digitale, comportano, come il GDPR dimostra in ogni sua prescrizione, un atteggiamento assai più attento a tutelare i valori fondamentali della libertà delle persone, garantendo il controllo sui loro comportamenti e la salvaguardia dei loro dati da usi illeciti o così invasivi da privare le persone di ogni effettiva libertà, spesso senza neanche garantire davvero nuove sicurezze.

15. Il mondo nuovo ha bisogno un diritto che di molta più attenzione ai valori in gioco e alla loro tutela, in sostanza ha bisogno di un "diritto per valori".
Ma un "diritto per valori" ha a sua volta bisogno inevitabilmente di strutture di enforcement e di tutela delle legalità agili; capaci di adattare velocemente le regole al modificarsi delle situazioni; attente ad arginare gli sviluppi della tecnologia senza impedirne i progressi; capaci di tutelare le libertà, non negandole ma regolandole.
In questo quadro sono da temere tutti gli atteggiamenti che mettano al centro i divieti e i vincoli, anche perché spesso, come ha detto il giudice Calabresi in un importante Convegno dell'Osservatorio Giordano dell'Amore tenutosi a Milano l'11 ottobre 2017 dal titolo "*Fake news e allarme sociale*: *responsabilità non censura*", il mondo attuale, e tanto più quello digitale in evoluzione, non hanno bisogno di eventuali divieti imposti sulla base di una realtà in continuo cambiamento. Al contrario: hanno bisogno di chi sappia accompagnare la tumultuosa evoluzione della società salvaguardandone i valori fondamentali e agendo sempre in modo da non pregiudicare con i divieti di oggi i progressi di domani.
In una parola: in un mondo caratterizzato dal cambiamento accelerato e continuo non abbiamo bisogno di regole ma di regolatori e i regolatori di cui abbiamo bisogno non sono quelli che sanno meglio applicare regole formalistiche a realtà in continuo cambiamento ma quelli che sanno guidare, regolare, inseguire i cambiamenti, mettendo sempre al centro gli uomini e le donne e i loro diritti fondamentali, primo dei quali è

in assoluto la libertà degli esseri umani di scegliere e decidere in modo responsabile, sapendo valutare gli effetti delle loro decisioni e avendo sempre presente che di questi effetti sono responsabili a seconda del ruolo e dei poteri esercitati, e dunque possono in qualunque momento essere chiamati a rispondere.

Lette in questa prospettiva le Linee guida 04/2020 sono particolarmente importanti ed è interesse e dovere di tutti vigilare sulla loro attuazione e su come le Autorità sapranno interpretare il ruolo che esse stesse si sono date approvandole.

Insomma, la protezione dei dati personali e con essa le Autorità che ne sono garanzia sono all'inizio di una nuova stagione, entusiasmante e complessa, così come certamente entusiasmante ma anche molto complessa è la nuova fase nella storia del mondo che da anni stiano vivendo e che l'epidemia del Coronavirus ha accelerato ogni oltre previsione.