04/05/2020 10:24
Sito Web

Agenda Digitale
IL PRIMO GIORNALE SULL'AGENDA DIGITALE ITALIANA

Il contact tracing Apple e Google alla prova della normativa privacy Ue

LINK: https://www.agendadigitale.eu/sicurezza/privacy/contact-tracing-il-sistema-di-apple-e-google-alla-prova-della-normativa-privacy-ue/

L'Exposure Notification Service di Google e Apple è, a oggi, coerente con la cornice normativa e regolamentare europea a tutela dei dati personali e della riservatezza dei cittadini. È indubbio tuttavia che i rischi legati a un simile sistema di tracciamento rimangano elevati. Vediamo quali sono e come superarli Nicola Sandon Associate di Tonucci & Partners Alessandro Vasta Partner, Tonucci & Partners In ambito europeo, l'impiego del sistema tecnologico di prevenzione e contrasto della pandemia da covid-19, sviluppato da Google ed Apple, dovrà necessariamente confrontarsi con la necessità di rispettare una serie di norme a tutela delle libertà personali del cittadino, tra le quali spiccano la Direttiva 58/2002 CE (ePrivacy) ed il Regolamento UE 2016/679 (GDPR). Stando alle dichiarazioni degli attori coinvolti, il sistema - denominato "Exposure Notification Service" ("ENS") - dovrebbe garantire un elevato grado di trasparenza e l'adozione di stringenti misure tecniche idonee a preservare la sicurezza e la riservatezza degli utenti. Prima di entrare nel merito del funzionamento di questo sistema e dell'approccio delle due big tech, è bene fugare ogni possibile dubbio: non vi è in programma alcuna release di un'applicazione di contact tracing "firmata" da Google ed Apple: esse si limiteranno a fornire il substrato tecnologico che consentirà una più efficiente ed efficace operatività delle soluzioni tecnologiche implementate a livello nazionale. Le due società inoltre hanno garantito che provvederanno alla completa dismissione del sistema, su base locale, al termine dell'emergenza. Indice degli argomenti Il progetto Con uno storico comunicato stampa congiunto rilasciato il 10 aprile scorso, Google ed Apple hanno annunciato al mondo di aver unito le proprie forze ai fini dello sviluppo di un sistema di tracciamento dei contatti, basato su tecnologia Bluetooth Low Energy (BLE), in grado di supportare le autorità sanitarie nazionali nel contenimento della diffusione del virus Covid-19 e agevolare il ritorno alla quotidianità nella fase post-emergenziale. In considerazione della situazione emergenziale e della vera e propria corsa allo sviluppo di applicazioni di contact tracing ad oggi in atto a livello globale, l'ambizioso progetto dei due colossi della Silicon Valley si struttura in due distinte fasi. La prima prevede il rilascio di apposite interfacce di programmazione delle applicazioni (API) che consentiranno l'interoperabilità tra i dispositivi smart recanti sistemi operativi Android e iOS. Google ed Apple hanno già avuto modo di chiarire come le API saranno rese disponibili unicamente alle autorità pubbliche, sanitarie e governative, preposte allo sviluppo di applicazioni per la lotta alla pandemia ed a condizione che tali app garantiscano specifici - ma non meglio precisati - requisiti in termini di privacy e sicurezza. Il rilascio ufficiale delle API - rese disponibili in versione beta ad un limitato gruppo di selezionati sviluppatori già al lavoro per conto delle autorità sanitarie pubbliche il 28 aprile scorso - è fissato per la metà del mese di maggio. Come sia il Comitato Europeo per la

Agenda Digitale.eu
IL PRIMO GIORNALE SULL'AGENDA DIGITALE ITALIANA

privacy e sicurezza. Il rilascio ufficiale delle API - rese disponibili in versione beta ad un limitato gruppo di selezionati sviluppatori già al lavoro per conto delle autorità sanitarie pubbliche il 28 aprile scorso - è fissato per la metà del mese di maggio. Come sia il Comitato Europeo per la Protezione dei Dati Personali ('EDPB') che la Commissione Europea hanno avuto modo di sottolineare, la realizzazione di piattaforme interoperabili costituisce un requisito indispensabile per garantire l'efficienza del contact tracing effettuato mediante mezzi digitali, soprattutto in un contesto, come quello comunitario, caratterizzato dalla libera circolazione delle persone: l'intervento in prima persona delle due società titolari dei due sistemi operativi più diffusi sul pianeta contribuirà in maniera decisiva alla soluzione di questa problematica. Le nuove API non contribuiranno solo alla creazione di un'interfaccia unica a livello globale, ma consentiranno probabilmente anche di eliminare alcuni dei limiti tecnologici in grado di compromettere la funzionalità delle app di tracciamento dei contatti, ad esempio prevenendo il consumo eccessivo della batteria e permettendo, nei dispositivi iOS, il funzionamento del Bluetooth anche con l'applicazione in background. La seconda fase, di ben più ampia portata, vedrà l'integrazione della tecnologia di tracciamento direttamente nei sistemi operativi proprietari, mediante il rilascio di appositi aggiornamenti. La funzionalità di contact tracing diverrà così parte integrante dei nostri dispositivi, in grado di operare (previo assenso dell'utente) anche senza necessità di scaricare l'applicazione sviluppata dalle autorità locali. App che rimarranno ad ogni modo indispensabili anche nella nuova cornice, sia per garantire un adeguato controllo sulla veridicità delle informazioni caricate dai soggetti risultati positivi al virus, sia per una più efficace gestione del flusso di informazioni verso i soggetti esposti ad un contatto a rischio. Tale soluzione mira ad agevolare la massima diffusione della tecnologia di tracciamento, contribuendo in maniera significativa al raggiungimento della cosiddetta 'massa critica', ovverosia di quel numero minimo di utenti in grado di garantire il buon funzionamento del sistema di prevenzione e che vari studi individuano tra il 60 e l'80% della popolazione. Il funzionamento Il sistema si basa su un apposito protocollo Bluetooth, programmato per rilevare la prossimità rispetto ad altri dispositivi dotati della medesima tecnologia e consentire lo scambio di informazioni predeterminate tra questi ai fini della registrazione di eventuali contatti a rischio. In pratica, la tecnologia BLE (la medesima impiegata anche per il funzionamento delle AirPods) trasforma i dispositivi mobili in una sorta di radiofari, che trasmettono in continuazione un determinato segnale e al contempo ricercano i segnali provenienti da altri dispositivi. Il segnale che viene emesso è costituito da identificativi pseudonimi (delle stringhe di numeri casuali denominate 'Rolling Proximity Identifiers') che non contengono alcuna informazione direttamente riconducibile al dispositivo emittente, sono soggetti a cifratura e mutano in maniera automatica ogni 10-20 minuti. Questi identificativi vengono generati da una chiave crittografica (c.d. 'Rolling Proximity Identifier Key') che, a sua volta, deriva da una ulteriore chiave crittografica che cambia ogni 24 ore (la 'Temporary Exposure Key'). Ciò significa che non si potrà

Agenda Digitale.eu
IL PRIMO GIORNALE SULL'AGENDA DIGITALE ITALIANA

ricollegare il singolo Rolling Proximity Identifier ad un determinato dispositivo senza avere a disposizione la Temporary Exposure Key. Ma come funziona nel concreto la tecnologia sviluppata da Apple e Google? Lo smartphone trasmette i Rolling Proximity Identifiers utilizzando la tecnologia BLE e ricerca gli identificativi provenienti da altri eventuali dispositivi nel proprio raggio di azione. Ogni smartphone che capta un identificativo pseudo-casuale, lo registra e lo conserva in locale. La registrazione dell'identificativo avverrà solo se il contatto sarà caratterizzato da una distanza e da una durata tale (ad es. a meno di due metri per più di cinque minuti) da comportare un effettivo rischio di infezione, da calcolarsi sulla base di un apposito algoritmo. I parametri di durata e distanza saranno identificati sulla base delle risultanze delle ricerche scientifiche ad oggi disponibili sul COVID-19 e potranno in ogni caso essere modificati sulla base delle indicazioni delle singole autorità nazionali. L'introduzione nell'equazione del parametro della potenza del segnale radio ricevuto (Received Signal Strength Indication o RSSI) è una delle novità che caratterizzano la soluzione tecnologica proposta dalle società americane: tale elemento potrebbe significativamente contribuire e ridurre il rischio di falsi positivi (o negativi) derivante dai limiti tecnici della tecnologia BLE. Se un soggetto risulta positivo al virus, esso potrà, a propria discrezione, acconsentire all'upload del proprio set di chiavi crittografiche giornaliere generate nei giorni precedenti al contagio (cosiddetti Diagnosis Key) in un server centralizzato. Anche se nulla di specifico viene indicato in proposito dalla documentazione tecnica ad oggi fornita da Google ed Apple, è probabile che il server che raccoglierà le Diagnosis Key verrà gestito direttamente dall'autorità sanitaria nazionale. Quali misure di sicurezza saranno applicate al server dipenderà dalla concreta implementazione del sistema. Il set di Temporary Exposure Keys che verrà inviato al server centralizzato, per lo meno attenendosi a quanto espressamente indicato dalla Commissione Europea nella propria 'Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection'[1], sarà composto delle chiavi generate nei 16 giorni precedenti all'accertata positività. L'upload delle Diagnosis Keys potrà avvenire unicamente previa acquisizione di esplicito e separato consenso degli utenti. Al fine di eliminare il rischio di falsi positivi, le società hanno inoltre indicato che la soluzione sarà sviluppata in modo da consentire l'invio dei dati al server centralizzato solo previa conferma della diagnosi da parte della competente autorità sanitaria (ad es. mediante assegnazione di un codice monouso da parte degli operatori sanitari). Inoltre, per poter procedere all'upload il soggetto risultato positivo dovrà necessariamente utilizzare l'applicazione nazionale. Almeno una volta ogni 24 ore le Diagnosis Key conservate nel server centralizzato verranno trasmesse a tutti gli smartphone parte della rete. Una volta entrati in possesso della chiave crittografica, i singoli dispositivi potranno avviare - in maniera del tutto automatica - un processo di decodifica dei Rolling Proximity Identifiers registrati sino a quel momento. Qualora la Diagnosi Key riesca ad 'aprire' la serratura di uno dei Rolling Proximity Identifiers conservati nella memoria locale del dispositivo, questo invierà un'apposita notifica al

Agenda Digitale.eu
IL PRIMO GIORNALE SULL'AGENDA DIGITALE ITALIANA

soggetto, comunicandogli che negli ultimi (16) giorni è stato soggetto ad un contatto a rischio. Da qualche indiscrezione, pare che ad oggi il sistema sia studiato per informare l'utente della data del contatto e della durata dello stesso: questo però andrebbe in diretto contrasto con le linee guida della Commissione Europea[2]. È curioso sottolineare come la soluzione proposta preveda che il 'match' tra Diagnosis Keys e identificativi pseudonimi avvenga integralmente all'interno del dispositivo mobile: in questo modo nessuno tranne l'utente sarà a conoscenza del match, né Google, né Apple, né la stessa autorità sanitaria. Interrogate sul punto, le società hanno poi rappresentato che in caso di disinstallazione dell'app sanitaria il database di Rolling Proximity Identifiers conservati nel dispositivo verrà automaticamente cancellato. Non è chiaro se tale soluzione verrà prevista, una volta entrati nella seconda fase del progetto, anche in caso di disattivazione della funzione nativa di contact tracing.

Perché il contact tracing?

Appare ormai evidente come la tecnica di tracciamento dei contatti sia stata individuata dalle autorità governative (e sanitarie) mondiali come una valida misura atta a prevenire e contenere la diffusione del coronavirus, soprattutto in una fase di allentamento delle misure restrittive come quella che auspicabilmente inizieremo a vivere a breve nel continente europeo. Scopo precipuo dell'attività di contact tracing è quello dell'interruzione della catena di trasmissione, mediante la tempestiva notifica della possibile esposizione a soggetti poi risultati positivi e la conseguente adozione di idonee misure di contenimento (quali l'auto-isolamento, la sottoposizione del soggetto a rischio al tampone, ecc.). Il tracciamento dei contatti viene ad oggi effettuato in maniera manuale dagli operatori sanitari, nel rispetto degli standard individuati dallo European Center for Disease Prevention and Control[3], con grande dispendio in termini di tempo e risorse, nonché con un grado di efficienza necessariamente commisurato alla capacità del singolo soggetto infetto di ricostruire i propri contatti risalenti fino a due settimane prima dell'intervenuta positività.

Come indicato dal Commissario straordinario per l'attuazione e il coordinamento delle misure di contenimento e contrasto dell'emergenza epidemiologica COVID-19, l'impiego della tecnologia in ambito di contact tracing appare in grado di 'dare un contributo rilevante per un tracciamento di prossimità molto più efficiente e rapido di quello tradizionale'[4], nonostante i (legittimi) dubbi da più parti sollevati in merito alla concreta efficienza di tali soluzioni, a causa della presenza di molteplici fattori che potrebbero facilmente determinarne il fallimento (quali l'elevata percentuale di soggetti che dovrebbero scaricare le app preposte a tal fine o la definizione di quali siano effettivamente i contatti da ritenersi "a rischio" in termini di prossimità e durata). Il tutto senza dimenticare che l'impiego della tecnologia di tracciamento non potrà in ogni caso sostituirsi al tracciamento manuale, ma dovrà a questo offrire supporto, collocandosi nel quadro di una ben più ampia strategia di contrasto e contenimento dell'epidemia che dovrà essere varata e diligentemente gestita dalle autorità nazionali.

La posizione europea in materia di contact tracing

Da un mese a questa parte si sono succeduti gli interventi di varie istituzioni europee dedicati all'impiego di applicazioni mobili e tecnologie di contact tracing

Agenda Digitale.eu
IL PRIMO GIORNALE SULL'AGENDA DIGITALE ITALIANA

nell'ambito della lotta al coronavirus, con il fine di contribuire - mediante l'impiego di cosiddetta soft law, ossia di disposizioni non legalmente vincolanti - allo sviluppo di un approccio comunitario sul tema, esponendone le criticità e fornendo indispensabili indicazioni in merito alle misure da adottare per la costruzione di soluzioni conformi alla vigente cornice normativa in materia di data protection. Degne di note, da ultimo, le posizioni della Commissione Europea, con la già citata guida dello scorso 16 aprile, e del EDPB, con le linee guida n. 4/2020 del 21 aprile scorso. Come si colloca dunque la soluzione proposta delle due società americane in questo panorama? In maniera forse inaspettata, il sistema di tracciamento dei contatti made in 'big tech' sembra offrire alcune garanzie di conformità al principio di protezione dei dati fin dalla progettazione (privacy-by-design) e per impostazione predefinita (privacy-by-default), nonché ai principi fondamentali sino ad ora elaborati a livello europeo, seppur con le dovute precisazioni. Innanzitutto, la scelta della tecnologia BLE rispecchia pienamente le indicazioni fornite da Commissione Europea e EDPB, che si sono da subito espressi in maniera piuttosto netta in favore dell'impiego di tale soluzione, in quanto essa da un lato appare in grado di offrire maggiori garanzie in materia di precisione - e dunque qualità - della rilevazione, e dall'altro, basandosi sul trattamento dei dati di prossimità, consente di evitare l'utilizzo di dati di localizzazione (raccolti ad es. mediante il GPS), poco funzionali e non strettamente necessari rispetto alla finalità del trattamento. Il sistema è stato poi ideato per essere completamente su base volontaria: nella seconda fase di sviluppo, quando la tecnologia verrà integrata nei sistemi operativi dei dispositivi mobili, la funzionalità di contact tracing sarà attivabile unicamente con il consenso dell'utente e potrà essere disabilitata in ogni momento. Si tratta di un principio più volte ribadito dalle istituzioni europee, e da ultimo ripreso dall'EDPB, il quale ha espressamente affermato che le persone che non intendano o non possano utilizzare tali tecnologie 'non dovrebbero subire alcun pregiudizio'. Particolare attenzione è stata inoltre dedicata dagli sviluppatori al rispetto del principio di minimizzazione dei dati, elemento cardine delle analisi effettuate dalle istituzioni europee e che trova ampia applicazione nell'ambito della soluzione di Google e Apple. In primo luogo, il sistema non utilizza in nessun caso dati direttamente identificativi, ma sempre dati pseudonimizzati mediante l'impiego di avanzate tecniche di cifratura, rendendo altamente residuale il rischio di risalire ad una persona identificabile anche in caso di data breach, e questo sia a livello di comunicazione tra dispositivo e dispositivo sia tra dispositivo e server centralizzato. In secondo luogo, il sistema si basa su una struttura completamente decentralizzata, che prevede l'invio di dati, sempre criptati, all'esterno dei singoli dispositivi unicamente in caso di riscontrata positività dall'utente al virus e solo previo ulteriore, esplicito consenso dello stesso. Come già indicato, non appare invece pienamente in linea con il principio di minimizzazione la scelta di condividere con il soggetto cui viene notificato il contatto a rischio la data e la durata dello stesso, in quanto tali elementi potrebbero consentire al destinatario della notifica di inferire l'identità del soggetto infetto. A valle degli ultimi chiarimenti forniti dalle società, anche il meccanismo di notifica appare conforme alle

Agenda Digitale
IL PRIMO GIORNALE SULL'AGENDA DIGITALE ITALIANA

indicazioni fornite dalla Commissione: il sistema prevede infatti la possibilità di invio automatico del messaggio di allerta solo previa approvazione e/o conferma da parte dell'autorità sanitaria. Viene dunque esclusa l'eventualità di decisioni basate esclusivamente su un processo automatizzato. Un elemento che ad oggi invece non viene affrontato nei documenti ufficiali rilasciati dalle società, ma che dovrà senz'altro essere oggetto di attenzione nelle successive fasi di sviluppo, è il periodo di conservazione nei dispositivi degli identificativi pseudonimi raccolti in fase di rilevazione di prossimità: sulla base di quanto indicato dalla guida della Commissione, esso non dovrebbe essere superiore ad un mese dal momento della raccolta. Altro tema di fondamentale importanza è quello connesso all'impiego degli algoritmi sviluppati da Google ed Apple per garantire l'accuratezza dell'analisi di prossimità svolta dall'Exposure Notification Service: se da un lato infatti i progressi fatti nella programmazione potrebbero dare un apporto insostituibile al perfezionamento dell'attività di contact tracing effettuata mediante sistemi tecnologici, riducendo il rischio di falsi positivi legati ai limiti intrinseci della tecnologia BLE (si pensi ad esempio al contatto avvenuto tra due vicini di casa che, pur trovandosi a meno di due metri l'uno dall'altro per un tempo prolungato, rimangono sempre divisi da una solida parete), dall'altro le istituzioni europee sono chiare nell'indicare che 'gli algoritmi devono essere verificabili e devono essere soggetti a un riesame periodico da parte di esperti indipendenti' ed il loro funzionamento dovrebbe 'svolgersi sotto la stretta sorveglianza di personale qualificato'[5]. Ad oggi tale profilo non è stato affrontato in maniera né implicita né esplicita dalle società, tuttavia appare evidente che accordi in questo senso dovranno essere presi a livello comunitario o nazionale nel breve periodo, anche in considerazione del fatto che buona parte delle app di contact tracing europee verranno implementate entro la fine del mese di maggio. Si rileva poi come, nonostante con il comunicato stampa Google ed Apple si siano impegnate a rendere pubblica la documentazione tecnica relativa al sistema di tracciamento, nessuna espressa garanzia è stata data in merito al fatto che esso sarà effettivamente open-source, una best practice a più riprese suggerita a livello comunitario[6]. Infine, dubbi più che legittimi sorgono sulla corretta individuazione della titolarità del trattamento posto in essere mediante il sistema qui analizzato: se per le singole app sviluppate a livello nazionale è infatti plausibile ritenere - accogliendo gli spunti offerti dalla Commissione - che la titolarità del trattamento ricadrà sulla competente autorità sanitaria, lo stesso approccio non potrà adottarsi nel momento in cui la tecnologia di tracciamento diverrà parte integrante del sistema operativo di smartphone, tablet e smart watches, rendendo di fatto superflua l'installazione di un'app. Come indicato sia dalla Commissione che dall'EDPB tale elemento è indispensabile almeno per tre differenti ordini di ragioni: (a) garanzia di trasparenza del trattamento; (b) individuazione del soggetto tenuto all'adempimento degli obblighi previsti dal GDPR, soprattutto in materia di informazione e svolgimento dell'obbligatoria valutazione d'impatto sul trattamento dei dati[7]; (c) garanzia del corretto esercizio dei diritti da parte degli interessati. Va d'altronde ricordato che,

Agenda Digitale
IL PRIMO GIORNALE SULL'AGENDA DIGITALE ITALIANA

nonostante le imponenti misure di sicurezza adottate, oggetto di trattamento saranno comunque dati personali, se pur pseudonimizzati, rientranti pertanto nell'ambito di applicazione del GDPR, e non dati tecnicamente anonimi. Si considerano tali, infatti, quelle informazioni non più riferibili ad una persona fisica identificata o identificabile o che riguardano dati personali resi sufficientemente anonimi da impedire l'identificazione dell'interessato con uno sforzo 'ragionevole', ivi inclusa la potenziale identificabilità mediante individuazione (isolamento di una persona all'interno di un gruppo), correlabilità (correlazione di due record riguardanti lo stesso individuo) e inferenza (deduzione, con probabilità significativa, di informazioni sconosciute relative a una persona)[8]. Si auspica pertanto un intervento risolutivo delle competenti istituzioni europee in materia, che possa far luce sulla questione con largo anticipo rispetto all'avvio della seconda fase del progetto presentato da Apple e Google. Ad ogni modo, l'iniziativa dei colossi americani del tech è al momento ufficialmente sotto la lente d'ingrandimento della Commissione Europea, cui spetterà l'ultima parola in termini di adeguatezza del sistema rispetto alla cornice normativa comunitaria. I rischi connessi all'implementazione Se possiamo affermare, fatte ovviamente salve le precisazioni di cui sopra, che la soluzione sviluppata dai tech giants americani presenta caratteristiche promettenti in materia di tutela dei dati personali, dobbiamo dare però conto del fatto che l'effettivo impatto dell'Exposure Notification Service sui diritti e le libertà degli interessati potrà essere realmente valutato solo alla luce dalla concreta implementazione dello stesso, in primo luogo da parte delle singole autorità nazionali, ed in secondo luogo dalle stesse società sviluppatrici. La soluzione pensata da Google e Apple rappresenta infatti uno standard tecnologico, ovverosia uno strumento che - com'è logico - si caratterizza per una certa flessibilità applicativa, esponendosi a manipolazioni da parte dei soggetti che decideranno di implementarlo. Le preoccupazioni riguardano principalmente tre profili applicativi: la strutturazione e la localizzazione dei server centralizzati, con particolare riferimento alla tipologia di dati in essi conservati, alle misure da implementare per garantirne la sicurezza ed alla necessità di assoggettamento ad un efficace controllo di una competente Autorità Garante privacy; la necessità per le autorità nazionali - legata ad esempio alla presenza in seno all'app di funzionalità diverse ed ulteriori rispetto a quella di semplice contact tracing - di procedere alla raccolta di dati ulteriori rispetto a quelli di prossimità, anche per scopi del tutto legittimi, ma con possibile vanificazione delle misure applicate in tema di pseudonimizzazione; il rispetto da parte dei governi del principio di limitazione della finalità. Se infatti le API saranno rilasciate unicamente a favore delle autorità direttamente coinvolte nello sviluppo di app 'ufficiali' contro la diffusione del COVID-19, non esistono sufficienti garanzie che gli Stati si asterranno dall'impiegare la tecnologia messa a loro disposizione per finalità o in contesti diversi rispetto alle condizioni originariamente previste (si pensi all'indagine su un omicidio o alla ricerca di un latitante). In Francia, ad esempio, si è già giunti ad un'impasse, con il governo che ha esplicitamente richiesto ad Apple di intervenire sul

Agenda Digitale.eu
IL PRIMO GIORNALE SULL'AGENDA DIGITALE ITALIANA

proprio sistema operativo per consentire il funzionamento in backgroud dell'app di contact tracing transalpina 'StopCovid'. L'app, infatti, che non prevede l'implementazione delle API delle società americane, implementa un protocollo tecnico diverso da quello proposto dall'azienda di Cupertino, protocollo che a detta di Apple offre un grado inferiore di tutela per la privacy degli utenti, consentendo allo Stato di procedere alla re-identificazione degli utenti mediante le informazioni presenti nel server centralizzato. In un inaspettato capovolgimento di ruoli - di cui è difficile non cogliere l'ironia - Apple ha con fermezza negato tale possibilità, anche se è lecito domandarsi se tale scelta sia dettata da una genuina preoccupazione della Mela per la privacy dei cittadini francesi o, piuttosto, da fini prettamente utilitaristici legati ad una più ampia diffusione della propria soluzione tecnica. Ultima criticità degna di rilievo è quella legata al rispetto del principio di limitazione della conservazione: se tutte le istituzioni europee e nazionali si sono trovate concordi nello stabilire che le app di tracciamento (e la tecnologia sottostante) dovranno essere dismesse al termine della situazione emergenziale, non si può non notare come nessuno ad oggi sia in grado di indicare con precisione quando ciò avverrà, o comunque di individuare dei criteri sufficientemente oggettivi per poterlo stabilire a priori, con il concreto rischio che quanto sviluppato in una situazione emergenziale divenga con tempo parte integrante della nostra realtà. Si pensi al complesso di disposizioni di natura straordinaria adottate in Europa e nel mondo a seguito dell'attentato alle torri gemelle dell'11 settembre 2001 per contrastare l'emergenza legata al terrorismo: come ben ci viene ricordato ogni volta che saliamo su un aereo o entriamo in un museo, parte di quelle disposizioni non sono mai state eliminate. Starà alle singole autorità, nazionali e sovranazionali, garantire il puntuale rispetto di tale impegno. Conclusioni Sulla base delle informazioni ad oggi disponibili, e tenuto in debita considerazione che si sta trattando di quello che ad oggi rappresenta un progetto, senz'altro destinato a subire molteplici modifiche e variazioni prima di giungere alla concreta implementazione, l'Exposure Notification Service proposto da Google ed Apple appare ad oggi in sostanza coerente con la cornice normativa e regolamentare europea posta a tutela dei dati personali e della riservatezza dei cittadini degli Stati membri. Per quanto post Brexit rilevante, un simile giudizio trova riscontro nelle note positive espresse dall'Autorità di controllo UK (Information Commissioner's Office), la quale, con parere ufficiale del 17 aprile scorso[9], ha sottolineato come l'effort posto in essere testimoni come innovazione e protezione dei dati personali siano concetti complementari, e non necessariamente antitetici, rilevando l'analogia tra gli elementi fondanti dell'ENS ed il progetto europeo di studio in materia di tracciatura dei contatti denominato 'Decentralized Privacy-Preserving Tracing' ('DP-3T'). Anche Thierry Breton, commissario europeo per il mercato interno e i servizi, ha recentemente espresso favore per l'iniziativa, a seguito di un colloquio con il CEO di Apple, Tim Cook. Pur dando atto degli aspetti positivi sin qui evidenziati, è indubbio che i rischi correlati all'impiego di un sistema di tracciamento, come quello proposto da Google ed Apple, rimangano comunque elevati. Da tale

Agenda Digitale.eu
IL PRIMO GIORNALE SULL'AGENDA DIGITALE ITALIANA

consapevolezza, deriverà la necessità di un costante monitoraggio del sistema da parte delle autorità di competenti, in un'ottica di adeguato bilanciamento tra restrizioni di diritti fondamentali degli individui e possibili vantaggi ricavabili nella lotta alla pandemia.

_____
_____
_____

__ Commissione Europea, 'Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection'. Il documento è disponibile qui https://ec.europa.eu/info/sites/info/files/5_en_act_part1_v3.pdf). 'It is sufficient to communicate to them the fact that they have been in epidemiological contact with an infected person during the past 16 days. As noted above, data about the time and place of such contacts should not be stored. It is therefore neither necessary nor possible to communicate those data' (Commissione Europea, op. cit., p. 10). European Center for Disease Prevention and Control, 'Contact tracing: public health management of persons, including healthcare workers, having had contact with COVID-19 cases in the European Union - second update', dell'8 aprile 2020, disponibile qui https://www.ecdc.europa.eu/sites/default/files/documents/Contact-tracing-Public-health-management-persons-including-healthcare-workers-having-had-contact-with-COVID-19-cases-in-the-European-Union%E2%80%93second-update_0.pdf Ordinanza 10/2020 del Commissario Straordinario per l'attuazione e il coordinamento delle misure di contenimento e contrasto dell'emergenza epidemiologica COVID-19 del 16 aprile 2020, disponibile qui http://www.governo.it/sites/new.governo.it/files/CSCovid19_Ord_10-2020.pdf Comitato Europeo per la Protezione dei Dati Personali, 'Linee-guida 04/2020 sull'uso dei dati di localizzazione e degli strumenti per il tracciamento dei contatti nel contesto dell'emergenza legata al COVID-19' del 21 aprile 2020, disponibile qui https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042020-use-location-data-and-contact-tracing_en e p. 14 'the source code of the application [...] must be open [...], so that any concerned party can audit the code, and [...] contribute to improving the code, correcting possible bugs and ensuring transparency in the processing of personal data' e Commissione Europea, op. cit., p. 12 'the Commission recommends that the source code of the app should be made public and available for review'. Ex art. 35 del GDPR. Cfr. Comitato Europeo per la Protezione dei Dati Personali, op. cit., p. 6. Information Commissioner's Office, 'Apple and Google joint initiative on COVID-19 contact tracing technology' del 17 aprile 2020, disponibile qui https://ico.org.uk/media/about-the-ico/documents/2617653/apple-google-api-opinion-final-april-2020.pdf