Diritto e Giustizia
IL QUOTIDIANO DI INFORMAZIONE GIURIDICA

Contact tracing. Spunta il modello centralizzato globale nelle Linee Guida EDPB 4/2020

Avvocato Bianchi Deborah

EDPB *"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" adottate il 21 aprile 2020*

Indice:

GIUFFRÈ FRANCIS LEFEBVRE
Privacy | Governance | Social Policy | Condizioni generali di abbonamento | Note legali
© Giuffrè Francis Lefebvre S.p.A. - Capitale Sociale € 2.000.000 i.v. - Sede legale: via Busto Arsizio, 40 - 20151 Milano P.IVA 00829840156
Società a socio unico. Società soggetta alla direzione e coordinamento di Editions Lefebvre Sarrut S.A.
Associata Unione Stampa Periodica Italiana

1- Presentazione.
Le Linee guida EDPB 4/2020 sono state redatte per la Fase 2 COVID. Tuttavia la raccomandazione dell'utilizzo proporzionato dei dati non puo' rispettare la rapidita' di risposta richiesta dal sistema anti COVID. Pare piuttosto che il Comitato dei Garanti UE abbia preparato il vademecum per un nuovo tempo in cui saremo costretti a convivere con il virus. In questo lasso temporale indefinito si ammette l'esistenza di un server back-end contenente i dati identificativi randomizzati dei cellulari dei positivi e dei rispettivi contatti. In definitiva l'EDPB ammette un modello centralizzato globale allocato nella cornice tecnologica allestita congiuntamente da Apple e Google. La garanzia privacy? Sono tutti dati anonimizzati. Peccato che l'anonimato non esista ….

2- Contact tracing. Modello decentralizzato e modello centralizzato.
Il contact tracing puo' essere sviluppato secondo un modello decentralizzato unicamente in locale nei cellulari degli utenti oppure secondo un modello centralizzato ove i cellulari degli utenti dialogano con un server centrale back-end. L'eHealth Network ha stilato una relazione ad hoc intitolata "*Mobile applications to support contact tracing in the EU's fight against COVID-19. Common EU Toolbox for Member States"* 15.04.2020 in cui si descrivono perfettamente i due modelli.

Modello decentralizzato (tecnologia bluetooth)
I dati di prossimita' relativi ai contatti generati dall'app rimangono solo sul dispositivo (cellulare). Ogni smartphone si distingue per un codice identificativo generato in modo random e temporaneo. Quando lo smatphone incontra nel raggio di 1 metro e ottanta centimetri un altro dispositivo ne recepisce e memorizza il codice e viceversa. Cosi' ciascun cellulare allochera' al proprio interno una lista di codici identificativi corrispondenti a tutti i dispositivi incontrati. Lista che verra' "aperta" unicamente se il proprietario del telefono risulti positivo al COVID-19. L'apertura della lista e' di competenza dell'Autorita' Sanitaria che provvedera' a valutare caso per caso l'opportunita' o meno di spedire la notifica di autoporsi in quarantena per 14 giorni. Caso per caso perche' la tecnologia impiegata consente di stabilire il tipo di contatto in termini di prossimita' (piu' o meno vicino) e di durata (piu' o meno tempo). Cosi' potra' essere insignificante un contatto di un secondo sebbene vicinissimo (la persona che si incrocia sul marciapiede) mentre potra' indurre all'alert il contatto al limite del metro e ottanta ma sviluppatosi per molto tempo (es. il collega di ufficio).
Questa soluzione del modello decentralizzato risulta ideale per salvaguardare la privacy ma non altrettanto funzionale per la ricostruzione del modello epidemiologico. Infatti l'Autorita' sanitaria non avra' nessun accesso alle informazioni anonimizzate e aggregate sugli effetti del distanziamento sociale, sull'efficacia dell'app e sulla tendenza prossima della potenziale diffusione del virus. Inoltre l'eHealth Network fa notare che la persona raggiunta dall'alert potrebbe essere interessata a ricevere comunicazioni dall'Autorita' sanitaria al fine di approfondire meglio la propria situazione e quindi potrebbe essere opportuno inserire nell'app l'opzione per il proprietario del telefono di rendere palese il proprio numero. Ovviamente si tratterebbe di una modalita' "opt-in" che non violerebbe la privacy nelle comunicazioni in quanto fondata sulla scelta dell'interessato.

GIUFFRÈ FRANCIS LEFEBVRE
Privacy | Governance | Social Policy | Condizioni generali di abbonamento | Note legali
© Giuffrè Francis Lefebvre S.p.A. - Capitale Sociale € 2.000.000 i.v. - Sede legale: via Busto Arsizio, 40 - 20151 Milano P.IVA 00829840156
Società a socio unico. Società soggetta alla direzione e coordinamento di Editions Lefebvre Sarrut S.A.
Associata Unione Stampa Periodica Italiana

Modello centralizzato o Back-end server solution (tecnologia Bluetooth)
Questo modello si compone di due meccanismi contemporanei: il contact tracing tra smartphone tipico del modello decentralizzato a cui si unisce un data base centrale allocato su un server back-end contenente i codici identificativi corrispondenti ai cellulari dei positivi e dei loro contatti.
Quando il proprietario del telefono si scopre positivo permette all'Autorita' sanitaria di aprire la lista dei contatti e scaricarne la parte relativa agli ultimi 14 giorni sul server centrale. Ciascun telefono si collega a intervalli regolari al server back-end per verificare eventuali matching con i codici ivi inseriti. Se si verifica la combinazione tra il codice identificativo del telefono in perlustrazione con uno dei codici memorizzati sul server significa che l'incontro col soggetto positivo e' avvenuto. Quindi appare una notifica che avvisa di essere entrato in contatto con il virus. Poi segue un messaggio dell'Autorita' sanitaria che fornisce istruzioni sulle azioni da compiere (es.: autoporsi in quarantena, recarsi a fare il triage, ecc…).
Questo modello centralizzato risulta assai piu' complesso di quello decentrato e probabilmente anche a maggior rischio privacy. Non convince infatti l'idea di un data base centrale di tutti i codici dei positivi e dei relativi contatti perche' - sebbene siano codici random – sono comunque codici in qualche modo identificativi. Il codice random corrisponde a un cellulare. Il cellulare rivela l'identita' del proprietario senza grande sforzo investigativo ed ecco la magia: esce dal cappello a cilindro un bel data base epidemiologico con nomi e cognomi (!!!).
Guarda caso Apple e Google (eterni rivali) hanno congiuntamente proposto a titolo di contributo umanitario un sistema centralizzato con server back-end per superare il problema delle eventuali incompatibilita' tra i cellulari iOS ed Android nonche' per superare le difficolta' di cesure informative transfrontaliere che potrebbero ostacolare la ricostruzione delle catene epidemiche.

3- Il modello centralizzato transfrontaliero Apple-Google ammissibile solo con dati anonimi

I due giganti della tecnologia web hanno proposto non una app ma un sistema di interoperabilita' capace di assurgere allo stato di hub di tutte le apps di contact tracing di tutti i Paesi UE ed extraUE. In definitiva il nodo tecnologico anti-COVID a marchio Apple-Google controllerebbe l'andamento epidemiologico del globo occidentale. Il 10 aprile 2020 i due colossi hanno lanciato l'iniziativa piu' o meno in questi termini: "*a comprehensive solution that includes application programming interfaces (APIs) and operating system-level technology to assist in enabling contact tracing […] in May, both companies will release APIs that enable interoperability between Android and iOS devices using apps from public health authorities. These official apps will be available for users to download via their respective app stores*"
Si tratta dunque di una soluzione completa che include le interfacce di programmazione delle applicazioni (API) e la tecnologia a livello di sistema operativo per aiutare a consentire il contact tracing […] a maggio, entrambe le societa' rilasceranno API che consentono l'interoperabilita' tra dispositivi Android e iOS che utilizzano le apps delle autorita' sanitarie pubbliche. Il download a garanzia dell'interoperabilita' tra iOS ed

GIUFFRÈ FRANCIS LEFEBVRE
Privacy | Governance | Social Policy | Condizioni generali di abbonamento | Note legali
© Giuffrè Francis Lefebvre S.p.A. - Capitale Sociale € 2.000.000 i.v. - Sede legale: via Busto Arsizio, 40 - 20151 Milano P.IVA 00829840156
Società a socio unico. Società soggetta alla direzione e coordinamento di Editions Lefebvre Sarrut S.A.
Associata Unione Stampa Periodica Italiana

Android per gli utenti di queste apps ufficiali sara' possibile a partire dalla meta' di maggio nei rispettivi app stores.
E' stato particolarmente evidenziato dalle due societa' che il sistema non e' esso stesso una app di tracciamento dei contatti e Google e Apple almeno sul momento non stanno costruendo nessuna applicazione in quanto l'obiettivo attuale consiste nel permettere l'interoperabilita' tra le apps ufficiali basate sullo scambio di informazioni via Bluetooth Low Energy. In seguito i due colossi nel loro sistema presenteranno dei servizi aggiuntivi utili per il contenimento del virus.

Purtroppo non sappiamo molto piu' sulla titanica iniziativa che viene laconicamente spiegata in tre pagine di cui rimettiamo le immagini esplicative allocate alla seguente URL
https://blog.google/documents/57/Overview_of_COVID-19_Contact_Tracing_Using_BLE.pdf

GIUFFRÈ FRANCIS LEFEBVRE
Privacy | Governance | Social Policy | Condizioni generali di abbonamento | Note legali
© Giuffrè Francis Lefebvre S.p.A. - Capitale Sociale € 2.000.000 i.v. - Sede legale: via Busto Arsizio, 40 - 20151 Milano P.IVA 00829840156
Società a socio unico. Società soggetta alla direzione e coordinamento di Editions Lefebvre Sarrut S.A.
Associata Unione Stampa Periodica Italiana

Diritto e Giustizia
IL QUOTIDIANO DI INFORMAZIONE GIURIDICA

Alice and Bob meet each other for the first time and have a 10-minute conversation.

Bob is positively diagnosed for COVID-19 and enters the test result in an app from a public health authority.

A few days later...

Their phones exchange anonymous identifier beacons (which change frequently).

With Bob's consent, his phone uploads the last 14 days of keys for his broadcast beacons to the cloud.

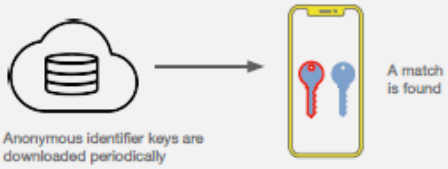
Google

Alice continues her day unaware she had been near a potentially contagious person.

Alice sees a notification on her phone.

Sometime later...

Alice's phone periodically downloads the broadcast beacon keys of everyone who has tested positive for COVID-19 in her region. A match is found with the Bob's anonymous identifier beacons.



Alice's phone receives a notification with information about what to do next.

Google

GIUFFRÈ FRANCIS LEFEBVRE

Privacy | Governance | Social Policy | Condizioni generali di abbonamento | Note legali

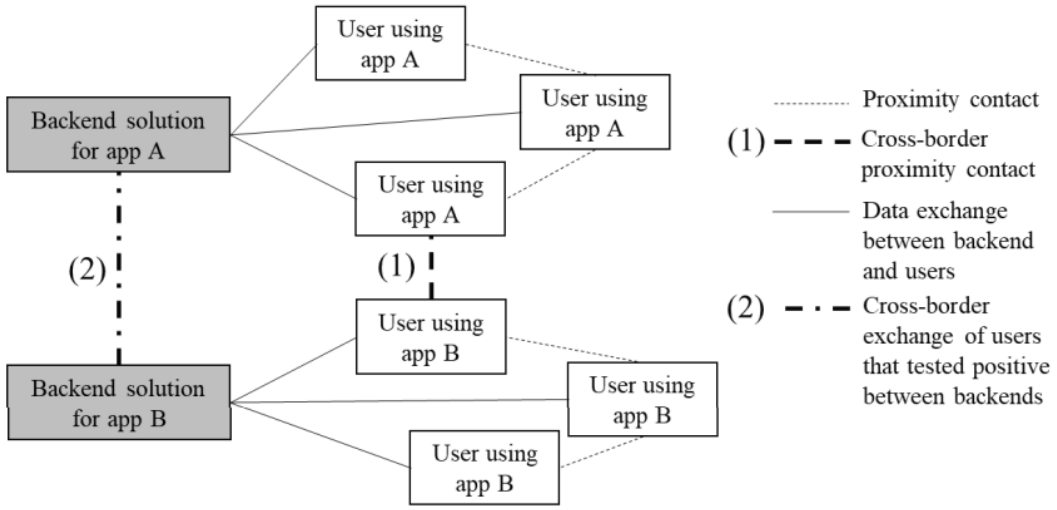
© Giuffrè Francis Lefebvre S.p.A. - Capitale Sociale € 2.000.000 i.v. - Sede legale: via Busto Arsizio, 40 - 20151 Milano P.IVA 00829840156
Società a socio unico. Società soggetta alla direzione e coordinamento di Editions Lefebvre Sarrut S.A.
Associata Unione Stampa Periodica Italiana

Il sistema Apple-Google – ove realizzato pedissequamente – costituira' "La Rete" del globo occidentale sull'andamento epidemiologico a cui tutti gli utenti, le istituzioni pubbliche e i vari stakeholders dovranno fare riferimento. Se ancora non fossero chiare le macro dimensioni del progetto, basti pensare che un sistema siffatto potra' costituire la piattaforma epidemiologica di elezione dell'OMS (!!!).
La misura del sistema Apple-Google si coglie piu' agevolmente guardandolo nella relazione di eHealth Network "*Mobile applications to support contact tracing in the EU's fight against COVID-19. Common EU Toolbox for Member States"* 15.04.2020 che lo adotta quale modello di interoperabilita' transfrontaliera. Nel punto c) della relazione rubricato "*Cross border interoperability requirements"* si osserva che le catene di trasmissione delle infezioni non si fermano ai confini nazionali o regionali e quindi le Autorita' sanitarie dovrebbero essere poste in grado di gestire anche a livello tecnologico tali catene di trasmissione transfrontaliere tramite apps e sistemi basati su protocolli dotati di almeno tre requisiti fondamentali:

1) allineamento dei criteri epidemiologici per definire contatti stretti per un'esposizione ad alto rischio, seguendo le indicazioni dell'OMS e dell'ECDC sui determinanti della tracciabilità dei contatti, inclusa la definizione di contatto stretto (distanza e durata dell'esposizione);
2) app di tracciamento dei contatti per registrare i contatti di prossimità di un utente con altri utenti utilizzando diverse app di tracciamento dei contatti (indicate come (1) nello schema seguente);
3) soluzioni di back-end, al fine di interrompere le catene di trasmissione transfrontaliere (indicate come (2) nel diagramma)

Eccettuato il primo requisito, il modello Apple-Google pare rispondere a quanto necessario. Il diagramma riportato di seguito descrive il sistema Apple-Google: i rettangolini bianchi rappresentano gli utenti e i loro dispositivi, dotati della app ufficiale dello Stato di appartenenza Sono in grado di registrare i contatti di prossimità e scambiare informazioni con il sistema back-end di riferimento (rettangolini grigi) che a propria volta comunica con un altro sistema back-end e cosi' via fino a coprire tutta la rete del globo occidentale.

GIUFFRÈ FRANCIS LEFEBVRE
Privacy | Governance | Social Policy | Condizioni generali di abbonamento | Note legali
© Giuffrè Francis Lefebvre S.p.A. - Capitale Sociale € 2.000.000 i.v. - Sede legale: via Busto Arsizio, 40 - 20151 Milano P.IVA 00829840156
Società a socio unico. Società soggetta alla direzione e coordinamento di Editions Lefebvre Sarrut S.A.
Associata Unione Stampa Periodica Italiana



[13] The contact tracing protocol released by Apple and Google on 10 April 2020 appears to address requirement 2) and 3). An example of a protocol covering Requirement 3 is the one established in the context of the Early Warning Response System (EWRS), which links the European Commission, ECDC and public health authorities in the EU and EEA countries responsible at national level for notifying alerts

Assunta la consapevolezza delle dimensioni globali del sistema Apple-Google non possiamo non preoccuparci della questione privacy auspicandosi che tutte le informazioni scambiate siano assolutamente anonime … ma esiste davvero l'anonimato?

4- Esiste davvero l'anonimato? Direttiva ePrivacy e GDPR: risposte diverse di fronte all'emergenza sanitaria.

L'anonimato nell'era dei data scientist è diventata una realta' in progressiva erosione destinata quasi a scomparire. Ormai l'anonimato inespugnabile è soltanto una chimera. La scienza della reidentificazione e della decanonizzazione è in grado di smantellare la maggior parte dei data base cosidetti anonimi o composti da dati aggregati.

Paul Ohm[1] nel saggio *"Broken promises of privacy: responding al surprising failure di anonymization"* 57 UCLA *Law Review* 1701 (2010) sostiene che *"un database, una volta rilasciato, puo' diventare piu' facile da reidentificare ma mai piu' difficile. Lunghe catene di inferenze da reidentificazioni passate non possono essere rotte con i progressi di domani".*

Dello stesso avviso quattro anni dopo il WP29 che nel Parere 5/2014 *"Tecniche di anonimizzazione"* https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf sostiene che *"di fatto, da un lato anonimizzazione e reidentificazione sono argomenti attivi di ricerca e vengono regolarmente pubblicate nuove scoperte in materia e, dall'altro lato, persino i dati resi anonimi, come le statistiche, possono essere utilizzati per arricchire i profili esistenti delle*

[1] Paul Ohm Professore associato presso la University of Colorado Law School. Questo articolo è stato presentato alla Conferenza degli studiosi sulla privacy e conferenze e seminari presso il Centro di Harvard per Research and Computer Science e Berkman Center, Princeton's Center for Information Technology Politica, Centro universitario Fordham per la politica legale e dell'informazione, Scuola dell'Università di Washington of Law, Dipartimento di Informatica e Ingegneria dell'Università di Washington, Informazioni sulla NYULaw Institute, DePaul Center for IP Law and Information Technology, International Association of Vertice sulla privacy globale dei professionisti della privacy e facoltà di giurisprudenza dell'Università del Colorado.

GIUFFRÈ FRANCIS LEFEBVRE
Privacy | Governance | Social Policy | Condizioni generali di abbonamento | Note legali
© Giuffrè Francis Lefebvre S.p.A. - Capitale Sociale € 2.000.000 i.v. - Sede legale: via Busto Arsizio, 40 - 20151 Milano P.IVA 00829840156
Società a socio unico. Società soggetta alla direzione e coordinamento di Editions Lefebvre Sarrut S.A.
Associata Unione Stampa Periodica Italiana

persone, determinando quindi nuovi problemi di protezione dei dati. L'anonimizzazione non va pertanto considerata un'operazione una tantum e i relativi rischi dovrebbero essere oggetto di un riesame periodico da parte dei responsabili del trattamento".

Se perfino le statistiche possono arricchire i profili delle persone risulta veramente poco rassicurante la garanzia che il modello centralizzato back-end processera' soltanto dati anonimi o piu' precisamente codici identificativi randomizzati.

Il legislatore europeo nella Direttiva ePrivacy del 2002 dimostra ingenuita' di fronte alla vera facies dell'anonimato mentre nel GDPR del 2016 ha assunto consapevolezza del problema.

La normativa sui dati di traffico dei cellulari e sui dati delle navigazioni internet rivela una certa fiducia nell'anonimato o nell'anonimizzazione quale misura di sicurezza privacy tombale. L'articolo 6 della Direttiva ePrivacy in merito ai dati sul traffico dei cellulari stabilisce che "*1. i dati sul traffico relativi agli abbonati ed agli utenti, trattati e memorizzati dal fornitore di una rete pubblica o di un servizio pubblico di comunicazione elettronica* ***devono essere cancellati o resi anonimi*** *quando non sono più necessari ai fini della trasmissione di una comunicazione, fatti salvi i paragrafi 2, 3 e 5 del presente articolo e l'articolo 15, paragrafo 1.*

L'articolo 9 sui *"Dati relativi all'ubicazione diversi dai dati relativi al traffico"* stabilisce che "*1. se i dati relativi all'ubicazione diversi dai dati relativi al traffico, relativi agli utenti o abbonati di reti pubbliche di comunicazione o servizi di comunicazione elettronica accessibili al pubblico* ***possono essere sottoposti a trattamento****, essi possono esserlo soltanto* ***a condizione che siano stati resi anonimi*** *o che l'utente o l'abbonato abbiano dato il loro consenso*"

L'impossibilita' di utilizzare unicamente dati anonimizzati nell'ingenuita' del legislatore del 2002 costituisce una limitazione dei diritti. Oggi sappiamo che anche l'utilizzo di dati anonimizzati può costituire una limitazione dei diritti quando sia possibile decodificarli e ricondurli all'interessato. E' l'articolo 15 della direttiva ePrivacy che nell'ipotesi in cui non si possa adottare l'anonimizzazione a causa di eventi di straordinaria necessita' ed emergenza che richiedono dati in chiaro, costringe il legislatore europeo a prevedere una legislazione di urgenza ad hoc a condizione che costituisca una "*misura necessaria, opportuna e proporzionata nell'ambito di una societa' democratica".*

Il GDPR 2016/679 dopo 14 anni di esperienza non crede più nell'efficacia garantista dell'anonimato o dell'anonimizzazione in quanto la maggior parte delle informazioni apparentemente non personali puo' essere ricondotta al corrispondente interessato. Pertanto il problema degli eventi straordinari viene affrontato con un atteggiamento disincantato rispetto all'anonimizzazione a cui si ricorre in extrema ratio prediligendo con lucida consapevolezza soluzioni di trattamento delle informazioni in chiaro opportunamente circoscritte nel contenuto e nella durata temporale (emergenza sanitaria eccezionale ex art. 9, 2, lett.i) GDPR 2016/679).

L'EDPB sostiene che il GDPR ha in se' gli strumenti per affrontare situazioni straordinarie come quella dell'epidemia COVID-19. Anzi – osserva l'EDPB - il GDPR fornisce i fondamenti legali che permettono ai datori di lavoro e alle autorità sanitarie di trattare dati personali ad alto impatto privacy quali quelli epidemiologici, senza necessita' di ottenere il consenso dell'interessato. Ovviamente, il fatto di trovarsi in siffatta emergenza non puo'giustificare un utilizzo arbitrario dei dati personali e quindi anche i trattamenti eseguiti

GIUFFRÈ FRANCIS LEFEBVRE
Privacy | Governance | Social Policy | Condizioni generali di abbonamento | Note legali
© Giuffrè Francis Lefebvre S.p.A. - Capitale Sociale € 2.000.000 i.v. - Sede legale: via Busto Arsizio, 40 - 20151 Milano P.IVA 00829840156
Società a socio unico. Società soggetta alla direzione e coordinamento di Editions Lefebvre Sarrut S.A.
Associata Unione Stampa Periodica Italiana

in emergenza devono rispettare al massimo i principi di minimizzazione, di essenzialita', di proporzionalita'.

5- Linee guida 4/2020 dell'EDPB: l'utilizzo proporzionato del dato nonostante l'emergenza sanitaria

Le Linee guida dell'EDPB 04/2020 sull'uso dei dati di localizzazione e degli strumenti per il tracciamento dei contatti nel contesto dell'emergenza legata al COVID-19 contemplano l'applicazione sia del modello decentrato sia del modello centralizzato con server back-end. Il modello decentralizzato ha un modesto impatto privacy mentre il modello centralizzato presenta un alto rischio privacy. Il purista della data protection opterebbe sicuramente per il modello decentralizzato escludendo qualsiasi ipotesi di costruzione di un data base centrale allocato su un server back-end altamente esposto ad attacchi di reidentificazione con effetti pregiudizievoli sulla vita delle persone. Tuttavia la ratio del superiore interesse pubblico della salute collettiva spinge ad ammettere un sistema composito misto in cui vi sia modello decentralizzato e centralizzato in quanto quest'ultimo e' importantissimo per ricostruire il modello epidemiologico svelandone le potenziali tendenze di diffusione.

Pertanto il Comitato dei Garanti UE ammette questo sistema misto centralizzato+decentralizzato su dati a cosi' alto impatto privacy a condizione che venga fatto un utilizzo proporzionato di questi dati. L'utilizzo proporzionato auspicato dal Comitato UE è una categoria mentis declinata secondo il quadrinomio "valutazione-azione-controllo-riaccomodamento". Così **l'utilizzo proporzionato dei dati sulla localizzazione dei positivi o dei "contattati" (local tracing) richiede un'anonimizzazione costantemente controllata** grazie all'imposizione dell'obbligo di renderne trasparente la metodologia ai titolari, ai responsabili privacy e ai controllori. Ammesso ormai che l'anonimato in senso assoluto non esiste, applicato un modo per interrompere il collegamento tra il dato e la persona occorre vigilarne costantemente la resilienza ad attacchi di reidentificazione sempre piu' sofisticati. La trasparenza del metodo usato per anonimizzare permette la verifica della permanenza dell'anonimato e l'immediato intervento di riaccomodamento nel caso si scoprisse la possibilita' di reidentificazione.

L'utilizzo proporzionato dei dati sui contatti (contact tracing) sempre secondo la sequenza "valutazione-azione-controllo-riaccomodamento" **richiede la preventiva valutazione di impatto** dell'app, **la minimizzazione** grazie a tecniche di privacy by default e privacy by design, **la crittografia** dei dati memorizzati e delle reti, **il regolare e frequente rinnovo dei codici identificatori** per scongiurare la relativa identificazione, **la pubblicazione del codice sorgente dell'algoritmo** per consentirne il controllo, **il tutto sottoposto alla valutazione umana che lungi dall'ammettere etichette da untore in via automatizzata verifica manualmente la segnalazione della macchina evitando falsi positivi ed effetti discriminatori inutili e lesivi della sfera individuale.**

L'EPDP conclude che l'utilizzo proporzionato dei dati significa responsabilita' nel trattamento secondo il concetto fondante di accountability in cui ciascun ruolo privacy (titolare, responsabile, incaricato) è chiamato a responsabilizzarsi rifuggendo dall'ossequio

GIUFFRÈ FRANCIS LEFEBVRE
Privacy | Governance | Social Policy | Condizioni generali di abbonamento | Note legali
© Giuffrè Francis Lefebvre S.p.A. - Capitale Sociale € 2.000.000 i.v. - Sede legale: via Busto Arsizio, 40 - 20151 Milano P.IVA 00829840156
Società a socio unico. Società soggetta alla direzione e coordinamento di Editions Lefebvre Sarrut S.A.
Associata Unione Stampa Periodica Italiana

statico della disciplina in un'attivita' dinamica di costante valutazione e riaccomodamento addirittura caso per caso ove necessario.
Lette queste raccomandazioni, non possiamo non evidenziare che in tempi di straordinaria emergenza sanitaria in cui la velocita' di risposta del sistema informativo puo' valere una vita umana, non c'è tempo per l'uso proporzionato del dato. E allora dobbiamo abdicare ai diritti privacy? Certamente no ma dobbiamo essere pratici: l'unica misura privacy possibile e' la cancellazione con termine di scadenza stabilito a priori. L'unica vera garanzia e' la prova di fronte ai nostri occhi che la lista dei codici identificativi viene azzerata ogni 14 giorni esclusa ogni latenza dei file log. L'unica vera garanzia è l'esclusione a priori del modello centrallizzato con server back-end fornito dalla "combinata" Apple-Google in quanto l'Europa è gia' dotata del modello EWRS (Early Warning and Response System) ovvero una piattaforma digitale servente il sistema transfrontaliero di allarme precoce e di scambio di informazioni in stati di rischio o minaccia di epidemia.
Piuttosto ci pare di avvertire nelle linee guida dell'EPDB una certa rassegnazione alla permanenza del sitema misto e del modello centralizzato anche dopo la fase 2 del COVID-19 quasi come si pensasse ad un osservatorio permanente.

6- Verso un modello centralizzato globale "*permanente*"?

Quanto durera' la Fase 2 del COVID-19? L'interrogativo e' legittimo alla luce dell'armamentario tecnologico messo in atto. Probabilmente dovremo abituarci a convivere con il virus per molto tempo e quindi anche il modello misto di local e contact tracing in allestimento ci accompagnera' per mesi. Dobbiamo quindi rassegnarci ad essere sottoposti – sebbene mediante codici identificativi randomizzati – al vaglio continuo del data base centrale dei positivi COVID-19. Ora le Linee guida dell'EPDB assumono un significato completo in quanto raccomandazioni non per una fase straordinaria in cui a causa della penuria di tempo è assai inverosimile assumere l'uso proporzionato dei dati bensi' raccomandazioni per una fase temporale indeterminata.
A maggior ragione ritorna la critica del purista della data protection: perche' fare un data base centrale di tutti i codici identificativi dei positivi e dei loro contatti? Si potra' obiettare che la permanenza di tali dati sul server dura 14 giorni e poi vengono cancellati. Tuttavia occorrerebbe la prova della cancellazione. Abbiamo visto che l'anonimato in definitiva non esiste e l'EDPB cerca di ovviare al problema raccomandando una sorveglianza continua contro gli attacchi di reidentificazione. Un tale controllo richiede risorse umane ed economiche. In un periodo di catastrofe economica mondiale sia concesso dubitare di investimenti tali per garantire la privacy dei cittadini.
Inoltre, come gia' accennato sopra, esiste gia' la piattaforma digitale transfrontaliera EWRS[2] gestita dall'ECDC dedicata a segnalare e a gestire gli stati di emergenza sanitaria europea. Addirittura dall'entrata in vigore dei regolamenti sanitari internazionali dell'OMS nel 2007 e dal nuovo quadro giuridico a livello dell'UE dal 2013, EWRS funziona anche in modo sempre più integrato con i suoi equivalenti dell'OMS e quindi assurge al monitoraggio della situazione globale del fenomeno epidemiologico. L'EWRS si collega anche ad altri sistemi come ad esempio, il sistema TessY che è un altro strumento

[2] Louise Bengtsson, Stefan Borg & Mark Rhinard (2018) "European security and early warning systems: from risks to threats in the European Union's health security sector", European Security,27:1,20-40,
DOI: 10.1080/09662839.2017.1394845

GIUFFRÈ FRANCIS LEFEBVRE
Privacy | Governance | Social Policy | Condizioni generali di abbonamento | Note legali
© Giuffrè Francis Lefebvre S.p.A. - Capitale Sociale € 2.000.000 i.v. - Sede legale: via Busto Arsizio, 40 - 20151 Milano P.IVA 00829840156
Società a socio unico. Società soggetta alla direzione e coordinamento di Editions Lefebvre Sarrut S.A.
Associata Unione Stampa Periodica Italiana

informatico utilizzato per la comunicazione di dati strutturati (basati su indicatori) di sorveglianza sulle malattie infettive elencate a livello dell'UE. Gli Stati membri sono tenuti per legge a comunicare periodicamente in TessY il livello di prevalenza della tubercolosi nella popolazione nazionale, secondo alcuni indicatori e definizioni di casi condivisi. Se un imprevisto aumento della tubercolosi viene rilevato in un determinato gruppo quando vengono raccolti tali dati TessY scattano le misure di sicurezza sanitaria. Ogni giorno la cabina di regia del virus costituita dalla squadra di intelligence epidemiologica tratta il problema in EWRS con gli aggiornamenti ed elabora previsioni sulle tendenze del fenomeno epidemico.
Abbiamo gia' la cabina di regia del virus, perche' dunque un data base centrale gestito da logiche automatizzanti? Il nostro purista della data protection non e' convinto e continua a pensare che l'aprioristica capacita' di discernimento dell'intelligenza artificiale ha ed avra' sempre bisogno della continua interazione umana per evitare la produzione di falsi positivi e per non incorrere in violazioni della privacy con effetti discriminatori.

GIUFFRÈ FRANCIS LEFEBVRE
Privacy | Governance | Social Policy | Condizioni generali di abbonamento | Note legali
© Giuffrè Francis Lefebvre S.p.A. - Capitale Sociale € 2.000.000 i.v. - Sede legale: via Busto Arsizio, 40 - 20151 Milano P.IVA 00829840156
Società a socio unico. Società soggetta alla direzione e coordinamento di Editions Lefebvre Sarrut S.A.
Associata Unione Stampa Periodica Italiana