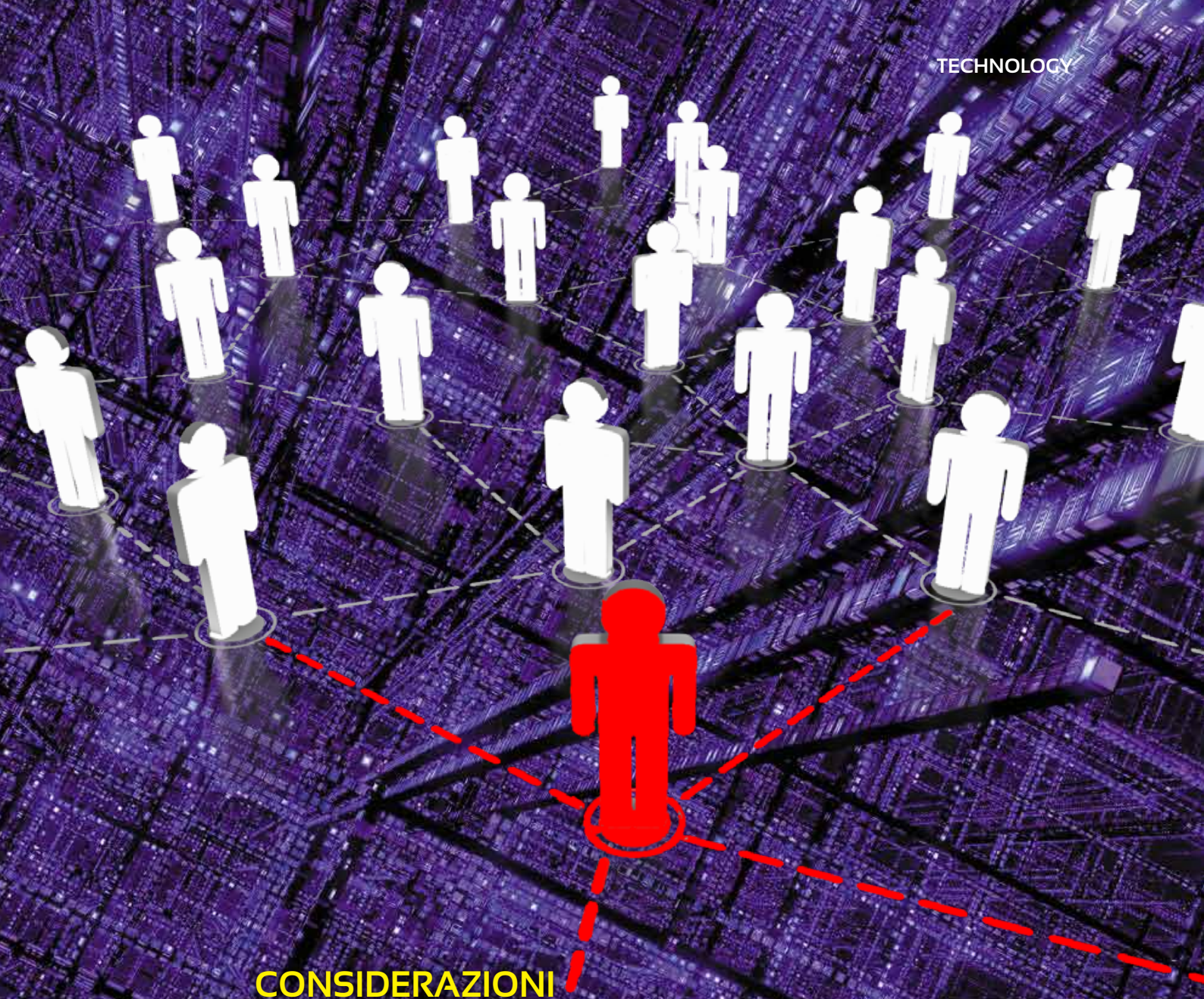

CONSIDERAZIONI SUL RUOLO DI APPLE E GOOGLE NEI SISTEMI DI CONTACT TRACING

L'impiego delle app si è notevolmente incrementato nel tempo, riproponendosi anche nel periodo emergenziale (determinato dall'insorgere e dalla diffusione del virus covid-19) come supporto alle autorità sanitarie nell'opera di contrasto alla pandemia nella prospettiva di interrompere la catena delle infezioni più rapidamente rispetto ad altre misure. Sotto questo profilo, il sistema di tracciamento dei contatti e allerta è stato ideato per individuare le persone entrate in contatto con soggetti che sono risultati contaminati dal virus e informarle sulle misure che andrebbero opportunamente assunte (autoisolamento, test, comportamenti da adottare se insorgono sintomi). Per queste ragioni, distintamente dalle comuni applicazioni, le tecnologie di rilevazione dei contatti (contact tracing) sono state annoverate tra le misure di sanità pubblica il cui scopo è la prevenzione e il contenimento della diffusione delle malattie infettive, in particolare nell'ambito della c.d. "fase 2" che ha avviato il ritorno alle normali attività economiche e sociali.

di Giovanni CREA, economista, è docente di "Economia aziendale e processi di amministrazione del lavoro" presso l'Università Europea di Roma. Dal 2008 è membro dell'Istituto Italiano per la Privacy e la valorizzazione dei dati, dove è Direttore della rivista di "Diritto, Economia e Tecnologie della Privacy".

1. Introduzione

La storia delle applicazioni informatiche, le c.d. *app* (abbreviazione di *application*, utilizzata in informatica) ci racconta che i software contenuti nei dispositivi personali sono stati progettati in funzione dell'interesse dei gestori a conoscere il comportamento degli utilizzatori; sotto questo aspetto, il software è sempre stato un mezzo di trattamento di dati impostato al fine di rilevare tale comportamento. Le *app*, dunque, sono state costruite secondo logiche tutt'altro che *data protection by design*, caratterizzandosi per il fatto di integrare istruzioni di elaborazione di dati e di trasmissione ad altre parti di informazioni su comportamenti e preferenze degli utenti, sulla loro localizzazione geografica, spesso senza che questi siano stati al corrente di ciò che avveniva con i dati a loro riferiti[1]. Esemplare, in tal senso, è il risalente caso del *software* denominato *Real player* – siamo negli anni novanta del secolo scorso – ideato per far accedere gli utenti a contenuti musicali e audiovisivi; oltre alla funzionalità di accesso, detta tecnologia conteneva un'istruzione che, a loro insaputa, trasmetteva al produttore le informazioni sui brani e sui video selezionati[2]. La scoperta di questo occulto trattamento di dati personali sollevò numerose critiche e proteste da parte delle associazioni di difesa dei diritti dei consumatori che, stando alle cronache dell'epoca, indussero il produttore a rimuoverla.

2. Sistemi di tracciamento e ruolo delle big tech

La realizzazione di un sistema di tracciamento dei contatti e allerta da parte di uno Stato si basa necessariamente sull'accesso a risorse tecnologiche rese disponibili da aziende che operano nel settore dell'*information and communication technologies*. L'esperienza europea su tale fronte – tra cui il sistema di tracciamento del nostro paese, istituito dall'art. 6 del D.L. 28/2020 (convertito con la L. 70/2020)[3] – si basa sul frame work tecnologico di *Exposure Notification*, sviluppato dalle società Apple e Google per supportare le applicazioni di tracciamento. Tra le altre iniziative delle due *big tech* si registra quella dell'azienda di Cupertino che ha aggiornato il proprio sistema operativo con la versione iOS 13.7 in cui ha integrato una funzione di rilevamento dei contatti per i paesi che non hanno ancora sviluppato un'applicazione per la notifica delle esposizioni. Il motore di ricerca, invece, realizzerà per il proprio sistema operativo (Android) un'applicazione 'standard' che verrà adeguata con le impostazioni fornite dai singoli paesi, ma che dovrà comunque essere scaricata dal Play Store.
Le cronache digitali hanno tratteggiato queste iniziative come una sorta di seconda fase di applicazione della modalità informatica di tracciamento, che tuttavia, con riguardo al nostro paese, non determina il superamento della soluzione di cui al citato art. 6[4] come anche dichiarato dai portavoce delle due aziende[5]. Al riguardo, va ricordato che l'art. 6, c. 5 del D.L. 28/2020 convertito prevede la titolarità pubblica della piattaforma (di cui l'apposita applicazione è una componente) con l'impiego di infrastrutture localizzate sul territorio nazionale, ove vengono effettuati i connessi trattamenti. In tale contesto il ruolo dei due operatori sembrerebbe limitato alla semplice fornitura di tecnologie, senza che questa implichi un trattamento di dati personali[6].

1 Sul punto, sia consentito un rinvio a G. Crea, Macchine intelligenti e protezione dei dati in una prospettiva di ethics by design, in Altalex, n. 5700, 20 febbraio 2018, reperibile all'indirizzo https://www.altalex.com/documents/news/2018/02/20/macchine-intelligenti-e-protezione-dei-dati-in-una-prospettiva-di-ethics-by-design

2 Cfr. G. Sartor, Il diritto della rete globale, in Ciberspazio e Diritto, vol. IV, n. 1, 2003, 67-94.

3 Cfr. Testo del decreto-legge 30 aprile 2020, n. 28, coordinato con la legge di conversione 25 giugno 2020, n. 70, in G.U. n. 162 del 29 giugno 2020.

4 Si veda, ad esempio, C. Rossi, App anti-Covid, arriverà la notifica di Apple-Google oltre Immuni, https://www.startmag.it/innovazione/app-anti-covid-oltre-immuni-arriva-la-notifica-di-apple-google/, 29 agosto 2020

5 Sul punto, si veda l'articolo di G. Tripodi, Immuni è qui per restare: l'app continuerà ad essere necessaria in Italia, https://www.mobileworld.it/2020/09/02/immuni-necessaria-in-italia-268092/, 2 settembre 2020.

6 Cfr. Garante per la protezione dei dati personali, Provvedimento di autorizzazione al trattamento dei dati personali effettuato attraverso il Sistema di allerta Covid-19 - App Immuni - 1° giugno 2020, Provvedimento n. 95/2020, https://www.garantepri-

Le soluzioni di Apple e Google pongono peraltro questioni rilevanti sotto il profilo della disciplina del trattamento dei dati personali, concernenti, in particolare, il ruolo che essi potrebbero svolgere nell'organizzazione del trattamento dei dati personali – ruolo che, invero, non appare tanto chiaro neppure nel modello organizzativo del sistema di *contact tracing* adottato nel nostro paese – ed i presumibili trasferimenti di dati personali verso il territorio degli Stati Uniti. Tali questioni riportano alla necessità di individuare misure tecniche e organizzative idonee a minimizzare i rischi di restrizione dei diritti e delle libertà delle persone fisiche che partecipano al tracciamento; rischi che possono derivare dall'integrazione dei due *provider* nel modello organizzativo del trattamento dei dati personali.

3. Profili organizzativi

Il coinvolgimento di Apple e Google nei trattamenti di dati associati al tracciamento dei contatti in altri paesi, considerate le caratteristiche del trattamento, le categorie di dati personali raccolti e, soprattutto, la capacità di controllo su tali dati dei due operatori ripropone, una volta di più, dilemmi etici e questioni di *compliance* alle norme del regolamento europeo (GDPR), delineando l'ombra di trattamenti occulti effettuati per finalità di controllo dei comportamenti e di aumento del potere di mercato[7]. Sappiamo come da simili trattamenti – tutt'altro che al servizio dell'uomo, come previsto dal GDPR[8] – possano derivare "probabili impatti" (rischi) su diritti, libertà, prerogative e interessi che regolano l'attività umana. Con riguardo a questi profili, il gruppo europeo dei garanti (EDPB) ci ricorda che nei casi in cui l'organizzazione del sistema di tracciamento coinvolge più figure devono essere definiti con chiarezza e fin dall'inizio i ruoli e le responsabilità di tali figure, prospettando che la titolarità dei trattamenti possa essere assegnata alle autorità sanitarie nazionali.
A queste valutazioni va aggiunta la considerazione circa l'opportunità di escludere le *big tech* anche da ruoli di responsabili del trattamento alla luce delle numerose esperienze che mostrano tutte le difficoltà derivanti dalla condizione di vincolare tali figure al titolare del trattamento trattando i dati personali soltanto su sua istruzione documentata. Tale scelta costituirebbe una misura di garanzia, riconducendo i relativi trattamenti alla base giuridica, rinvenibile nel diritto dell'Unione o in quello nazionale, che prevede finalità di interesse pubblico, in particolare nella sanità pubblica, evitando in tal modo alla radice lo svolgimento di trattamenti per finalità legate agli interessi dei due *provider*. Con riguardo a quest'ultimo aspetto il *board* europeo si richiama al principio di limitazione delle finalità (art. 5.1.b), GDPR) in virtù del quale le finalità devono essere sufficientemente specifiche in modo da escludere trattamenti ulteriori per scopi non legati all'emergenza causata dal Covid-19 (ad esempio, per fini commerciali)[9].

4. Implicazioni sui trasferimenti dei dati personali.

La prospettiva dell'inclusione di Apple e Google nell'organizzazione e gestione dei trattamenti dei dati di tracciamento pone anche la questione dei trasferimenti di tali dati personali verso il territorio degli Stati Uniti, in cui i due *provider* hanno sede. È ben noto, al riguardo, che questi trasferimenti vanno ora valutati alla luce della sentenza c.d. Schrems II[10] della Corte di giustizia UE che ha dichiarato invalida la Decisione 2016/1250 della Commissione europea. Con tale provvedimento l'autorità di Bruxelles aveva certificato l'adeguatezza della protezione dei dati personali stabilita dai principi adottati il 7 luglio 2016 dal Dipartimento del Commercio degli Stati Uniti e dalle dichiarazioni e impegni ufficiali riportati negli allegati alla decisione del 2016; principi e impegni che nel loro insieme formavano lo scudo

vacy.it/home/docweb/-/docweb-display/docweb/9356568

7 Cfr. F. Nicolicchia, Sorveglianza di massa e prerogative di riservatezza dell'individuo durante l'emergenza SARS-CoV-2. Scenari attuali e prospettive future, in www.giuri.unife.it/it/coronavirus/diritt
o-virale.

8 Si veda il quarto considerando del Regolamento (UE) 2016/679.

9 Cfr. 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, 21 aprile 2020, parr. 25-26.

10 Corte di giustizia Ue, Causa C-311/18, Data Protection Commissioner/Maximilian Schrems e Facebook Ireland, http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex
=0&doclang= IT&mode=lst&dir=&occ=first&part=1&cid=1946358

UE-U.S.[11]. I giudici di Lussemburgo hanno rilevato l'assenza del requisito della "sostanziale equivalenza" della normativa statunitense con il GDPR, con particolare riguardo sia all'accesso e utilizzo di tali dati da parte delle autorità interne previsto dalla suddetta normativa nel quadro dei programmi di sorveglianza a fini di sicurezza sia al meccanismo di mediazione previsto dallo stesso *Privacy shield*[12].
Peraltro, la mancanza di una decisione di adeguatezza del sistema statunitense di protezione dei dati personali apre alla valutazione della capacità degli strumenti giuridici contemplati dal GDPR all'art. 46, di garantire la protezione dei dati personali trasferiti oltreoceano secondo i canoni dello stesso regolamento. Sul punto va osservato come tale valutazione venga rimessa ai soggetti del trasferimento (l'esportatore e l'importatore dei dati) la cui indipendenza dalla normativa statunitense – in particolare, l'indipendenza della parte importatrice dei dati personali – appare difficilmente ipotizzabile, specie se raffrontata a una normativa che ha violato un accordo come il *Privacy shield* definito su scala geopolitica[13]. Sotto questo aspetto, ad esempio, lo strumento delle "clausole contrattuali standard" incontrerebbe difficoltà di applicazione, con particolare riguardo alla clausola n. 5, lett. b) che prevede la garanzia da parte dell'importatore "*di non avere motivo di ritenere che la normativa ad esso applicabile impedisca di seguire le istruzioni dell'esportatore o di adempiere agli obblighi contrattuali, e di comunicare all'esportatore, non appena ne abbia conoscenza, qualsiasi modificazione di tale normativa che possa pregiudicare le garanzie e gli obblighi previsti dalle presenti clausole, nel qual caso l'esportatore ha facoltà di sospendere il trasferimento e/o di risolvere il contratto;*"[14].

Casi come questi, dunque, mettono a dura prova la tenuta degli strumenti di cui all'art. 46, GDPR, richiedendo una valutazione (da parte dell'esportatore UE e dell'importatore extra UE) delle circostanze del trasferimento e dell'integrazione di eventuali misure aggiuntive; valutazione che non esclude la scelta di chi esporta i dati di sospendere o porre fine al loro trasferimento, aprendo alla prospettiva che i dati dei cittadini europei restino e vengano trattati sul territorio dell'Unione, in tal modo risolvendo alla radice il problema del trasferimento dei dati. Peraltro, tale scelta potrebbe essere riguardata alla stregua di una misura organizzativa da integrare nella valutazione d'impatto del trattamento sulla protezione dei dati ai sensi dell'art. 35, GDPR. Tanto più se si considera che i grandi *provider* d'oltreoceano hanno, tutti, uno stabilimento nell'UE. ©

11 Cfr. M. Masnada, Schrems II: invalido lo scudo UE-USA per la privacy ma valide le clausole contrattuali tipo per il trasferimento di dati extra UE, https://www.dirittobancario.it/sites/default/files/allegati/masnada_m._schrems_ii_la_sentenza_della_ corte_ue_sul_privacy_shield_2020.pdf La Corte ritiene che il requisito della "sostanziale equivalenza" della normativa U.S. con il diritto dell'Unione europea in materia di protezione dei dati personali non sia soddisfatto, sia con riguardo alle limitazioni alla protezione dei dati personali trasferiti dall'Unione oltre oceano derivanti dall'accesso e utilizzo di tali dati da parte delle autorità interne nel quadro dei programmi di sorveglianza previsti dalla suddetta normativa, sia in riferimento al meccanismo di mediazione previsto da tale decisione, all'indipendenza del mediatore e all'esistenza di norme che consentano a quest'ultimo di adottare decisioni vincolanti nei confronti dei servizi di intelligence statunitensi e delle altre autorità pubbliche statunitensi.

12 La Corte ritiene che le limitazioni che risultano dalla normativa degli Stati Uniti in materia di accesso e di utilizzo, da parte delle autorità interne, di dati trasferiti dall'Ue, non presentano i requisiti di proporzionalità previsti dal diritto unionale, giacché i programmi di sorveglianza fondati sulla suddetta normativa non si limitano a quanto strettamente necessario. Lo stesso collegio ha osservato che il meccanismo di mediazione previsto dal Privacy shield non fornisce alle persone interessate un mezzo di ricorso che offra garanzie sostanzialmente equivalenti a quelle previste nel diritto dell'Ue, tali da assicurare tanto l'indipendenza del mediatore quanto l'esistenza di norme che consentano al suddetto mediatore di adottare decisioni vincolanti nei confronti dei servizi di intelligence e delle autorità statunitensi.

13 Cfr. M. Nicotra, Addio Privacy Shield, perché è un grosso problema per le aziende e come affrontarlo, in Cybersecurity360, 17 luglio 2020, https://www.cybersecurity360.it/legal/privacy-dati-personali/addio-privacy-shield-perche-e-un-grosso-problema-per-le-aziende/

14 Sul punto si veda anche Corte di giustizia Ue, Causa C-311/18, cit., paragrafo 142.