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

Lotta al Coronavirus, Paese che vai privacy che trovi: i diversi approcci (Europa, Cina, Corea, Israele)

LINK: https://www.agendadigitale.eu/sicurezza/privacy/lotta-al-coronavirus-paese-che-vai-privacy-che-trovi-i-diversi-approcci-europa-cina-corea-is...

Lotta al Coronavirus, Paese che vai privacy che trovi: i diversi approcci (Europa, Cina, Corea, Israele) Home Sicurezza digitale Privacy Per far fronte al coronavirus, la Cina ha rafforzato il suo già massiccio sistema di sorveglianza. Corea del Sud e Israele, pur senza ricorrere al modello di Pechino, sembrano derogare al diritto alla privacy più significativamente di Italia e Europa, che scelgono un approccio più garantista. Un confronto fra i vari modelli 1 minuto fa Giuseppe Vaciago Partner R&P Legal e fondatore di Tech&Law Center Le emergenze mettono in luce la filosofia di Stato che c'è in un Paese. Per il contenimento della diffusione del coronavirus la Cina ha fortemente intensificato il suo sofisticato e criticato sistema di sorveglianza, con circa 200 milioni di telecamere di sicurezza installate in tutto il Paese, utilizzando specifiche applicazioni per la creazione di cluster di Big Data, al fine di far rispettare la quarantena ai pazienti infetti e per mappare i movimenti dei potenziali infetti e quindi del virus. La localizzazione e l'isolamento dei focolai grazie alle nuove tecnologie ha consentito di limitare fortemente il contagio. All'opposto, in Italia e in Europa si sta perseguendo invece un modello decisamente più garantista che limita solo in minima parte il perimetro del diritto alla privacy. Altri Paesi, invece - dalla Corea del Sud a Israele - scelgono una via di mezzo pur senza mettere in atto la massiccia sorveglianza cinese stanno decidendo di derogare al diritto alla privacy. Facciamo il punto sui diversi approcci. Indice degli argomenti I provvedimenti italiani per far fronte all'emergenza Il "modello italiano" in materia di circolazione di dati personali Il progetto Baseline di Google I modelli sudcoreano e israeliano Gdpr e direttiva ePrivacy Conclusioni I provvedimenti italiani per far fronte all'emergenza In Italia la prima interessante norma in materia di dati personali nell'ambito della emergenza sanitaria è stata emanata con il Decreto-Legge del 9 marzo 2020, n. 14 Disposizioni urgenti per il potenziamento del Servizio sanitario nazionale in relazione all'emergenza COVID-19 in Gazzetta Ufficiale con il numero di serie generale n.62 del 09 marzo 2020, in vigore dal 10 marzo 2020. Il decreto, con cui sono state previste una serie di disposizioni immediatamente applicabili al Sistema Sanitario, all'art.14 indica anche alcune disposizioni in materia di trattamento dei dati personali nel contesto emergenziale, come già illustrato nell'articolo di Agenda Digitale. Il comma 1 prevede che fino al termine dello stato di emergenza deliberato in data 31 gennaio 2020, per motivi di interesse pubblico nel settore della sanità pubblica e, in particolare, per garantire la protezione dall'emergenza sanitaria a carattere transfrontaliero mediante adeguate misure di profilassi, nonché per assicurare la diagnosi e l'assistenza sanitaria dei contagiati ovvero la gestione emergenziale del SSN, i soggetti operanti nella Protezione civile, gli uffici del Ministero della salute e dell'Istituto Superiore di Sanità, le strutture pubbliche e private che operano nell'ambito del SSN ed in generale tutti i soggetti coinvolti nella emergenza

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

come elencati al DPMC del 05/03/2020, "anche allo scopo di assicurare la più efficace gestione dei flussi e dell'interscambio di dati personali, possono effettuare trattamenti, ivi inclusa la comunicazione tra loro, dei dati personali, anche relativi agli articoli 9 e 10 del GDPR, che risultino necessari all'espletamento delle funzioni attribuitegli nell'ambito dell'emergenza determinata dal diffondersi del Covid-19". Questi trattamenti vengono effettuati, secondo quanto previsto dal DL, nel rispetto del GDPR e nello specifico degli articoli 9, paragrafo 2, lettere G (motivi di interesse pubblico), H (medicina preventiva) e I (motivi di interesse pubblico nel settore della sanità pubblica), e dell'articolo 10 (trattamento dei dati personali relativi a condanne penali e reati), nonché nel rispetto del Codice della Privacy, come modificato dal DLgs. 101/18, articolo 2 sexies, comma 2, lettere T (attività amministrative e certificatorie correlate a quelle di diagnosi, assistenza o terapia sanitaria o sociale) ed U (compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario, nonché compiti di igiene e sicurezza sui luoghi di lavoro e sicurezza e salute della popolazione, protezione civile, salvaguardia della vita e incolumità fisica). Al comma 2, inoltre, è previsto che la comunicazione dei dati personali a soggetti pubblici e privati, diversi da quelli di cui al comma 1, nonché la diffusione dei dati personali diversi da quelli di cui agli articoli 9 e 10 del GDPR, è effettuata, nei casi in cui risulti indispensabile ai fini dello svolgimento delle attività connesse alla gestione dell'emergenza sanitaria in atto. È significativo, in ultimo, che il decreto preveda che, avuto riguardo alla necessità di contemperare le esigenze di gestione dell'emergenza sanitaria in atto con quella afferente alla salvaguardia della riservatezza degli interessati, i soggetti di cui al comma 1 possono conferire le autorizzazioni di cui all'articolo 2 quaterdecies del Codice Privacy con modalità semplificate, anche oralmente. Quest'ultima norma ha, infatti, introdotto, una figura ulteriore rispetto all'incaricato previsto dall'art. 19 GDPR, ossia una persona fisica espressamente designata a cui titolare e responsabile possono assegnare, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, specifici compiti e funzioni connessi al trattamento di dati personali. Il titolare o il responsabile individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta. Il "modello italiano" in materia di circolazione di dati personali Dunque, operativamente in Italia è consentito agli enti impegnati a far fronte della emergenza, di operare trasferimenti di dati tra di loro senza scopi specifici se non l'emergenza stessa, e all'esterno a soggetti pubblici o privati solo ai fini dello svolgimento delle attività connesse all'emergenza sanitaria. Inoltre, l'interessato - che a questo punto non è necessariamente contagiato o malato ma in generale chiunque coinvolto- può essere informato del trattamento in modalità semplificata anche oralmente. In ultimo, gli enti previsti dal comma 1 possono designare specifiche figure autorizzate ad operare questo tipo di interscambio o flusso di dati personali sanitari. WHITEPAPER Data Strategy: quali sono le 3 fasi principali del processo di relazione con il cliente? Big Data Big Data Scarica il Whitepaper La norma appare basilare e necessaria, soprattutto in Lombardia, dove il personale sanitario in

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

queste ore è messo a dura prova dal crescente numero di contagi e non sarebbe nelle condizioni di far fronte ad alcune garanzie previste dal GDPR come implementato dal DLgs. 101/2018. Stiamo comunque assistendo ad un susseguirsi di provvedimenti, quindi non è detto che questo tipo di regolazione emergenziale rimanga in vigore in questi termini a lungo. In queste ore, il cosiddetto "modello italiano" sembra aver ispirato non soltanto l'approccio di altri sistemi sanitari, ma anche per quanto riguarda la previsione di alcune norme specifiche in materia di circolazione di dati personali. Sul punto, infatti, nonostante dalle dichiarazioni del Governo britannico sembrerebbe che l'approccio per far fronte alla pandemia si discosti dalle misure adottate nel Belpaese dal punto di vista sanitario, l'ICO (Autorità Garante nel Regno Unito) ha pubblicato sul proprio sito alcune FAQ in cui viene anzitutto precisato che le leggi sulla protezione dei dati e sulle comunicazioni elettroniche non impediscono al Governo, al Sistema sanitario nazionale o a qualsiasi altro operatore sanitario di inviare messaggi di salute pubblica alle persone, per telefono, SMS o e-mail, poiché questi messaggi non sono di marketing diretto. In secondo luogo, viene precisato che le stesse leggi non impediscono di utilizzare le più recenti tecnologie per facilitare consultazioni e diagnosi sicure e rapide. Gli enti pubblici possono richiedere un'ulteriore raccolta e condivisione di dati personali per proteggersi da gravi minacce alla salute pubblica. Il progetto Baseline di Google Negli Usa dove, nonostante la proposta di legge di qualche settimana fa di due senatrici non esiste a tutt'oggi una Autorità Garante per la Privacy federale nonostante su questi temi in Nord America si sia sempre mostrato un approccio meno garantista rispetto a quello europeo, sembrerebbe che si stia per adottare un sistema in grado di creare una crasi dei due modelli, quello italiano che consente la circolazione dei dati ma di fatto solo tra gli addetti ai lavori, e quello cinese che sembrerebbe avere sacrificato, e di molto, alcuni importanti principi in materia di protezione dei dati personali. Venerdì 13 marzo 2020 nel corso di una conferenza stampa è stato dichiarato lo stato di emergenza nazionale ed è stato annunciato che Google starebbe lavorando allo sviluppo di un sito web di screening attraverso il quale le persone potranno compilare un questionario e comprendere come ottenere un test per il coronavirus. Il sito web dovrebbe avere una serie di opzioni per conoscere i fattori di rischio e i sintomi del coronavirus. Nello specifico ha dichiarato Sundar Pichai (CEO di Google), man mano che diventeranno disponibili altri kit per il test, vi sarà un percorso per la salute pubblica e le agenzie sanitarie per indirizzare le persone verso il sito web Baseline, in cui gli individui più a rischio potranno essere indirizzati ai siti delle autorità pubbliche sanitarie locali. Il progetto Baseline, va precisato, è un'ambiziosa iniziativa a lungo termine di Alphabet per raccogliere in modo anonimo informazioni genetiche e molecolari da centinaia di persone per creare una mappa dettagliata, o baseline, di ciò che dovrebbe essere un essere umano sano. È un progetto avviato nel 2014 come uno dei progetti di Google, ed è guidato da Andy Conrad, e non sembrerebbe essere stato creato ad hoc per affrontare l'emergenza sanitaria. Baseline, infatti, avrebbe il dichiarato compito di "costruire la prossima generazione di strumenti e servizi sanitari" ed è stata definita come un'iniziativa

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

in grado di mappare i punti di dati sanitari utilizzati nella ricerca clinica e tale ricerca viene utilizzata in collaborazione con altri ricercatori, clinici, ingegneri, progettisti e volontari. I modelli sudcoreano e israeliano In Sud Corea, uno dei primi Paesi costretti a far fronte alla emergenza sanitaria dopo la Cina, è stata utilizzata una app per smartphone. L'app, sviluppata dal Ministero dell'Interno e della Sicurezza, permette a chi ha ricevuto l'ordine di non uscire di casa di rimanere in contatto con gli assistenti sociali e di riferire i propri progressi. Mediante l'app viene utilizzato anche il GPS per tenere traccia della loro posizione per assicurarsi che non stiano violando la quarantena. Il servizio, denominato "auto-quarantena di sicurezza", è stata lanciato per gli smartphone Android, mentre la versione per iPhone dovrebbe essere rilasciata il 20 marzo. I funzionari hanno detto che è destinato ad aiutare a gestire il crescente carico di casi e a prevenire i casi di "super untori". Secondo le attuali linee guida dei centri coreani per il controllo e la prevenzione delle malattie, chiunque sia entrato in contatto con un portatore di coronavirus confermato è soggetto ad un'auto-quarantena obbligatoria di due settimane. Per "contatto" si intende l'essere stato a meno di due metri da un portatore confermato, o l'essere stato nella stessa stanza dove un paziente confermato ha mostrato sintomi del virus (quali ad esempio, tosse, febbre o mal di gola). Una volta che i soggetti in auto-quarantena ricevono un ordine dal loro centro medico locale, è legalmente vietato loro di lasciare le aree di quarantena - di solito le loro case - e sono istruiti a mantenere una rigorosa separazione dalle altre persone, compresi i familiari. I soggetti in isolamento sono assegnati a un funzionario del governo locale, che controlla telefonicamente due volte al giorno lo sviluppo di eventuali sintomi. Al contempo, su tutto il territorio nazionale sudcoreano, le squadre di test mobili sono dispiegate per raccogliere campioni in caso di escalation. Di fatto, anche in Sud-Corea, l'interessato dalle norme di prevenzione che derogano alla consueta tutela della privacy, sembrano riguardare non solo coloro che hanno effettivamente contratto il virus ma tutti i soggetti potenzialmente pericolosi per l'espandersi della malattia. In ultimo, anche Israele sembrerebbe voler ricorrere a sistemi di geolocalizzazione per far fronte alla pandemia. Il primo ministro, il 14 marzo 2020, dopo aver dichiarato lo stato di emergenza e aver imposto restrizioni severe oltre che aver chiuso scuole, università, bar e ristoranti ed aver proibito i raggruppamenti di più di 10 persone, ha dichiarato di voler utilizzare i sistemi di sorveglianza tecnologica che i servizi segreti interni, usano «nella guerra al terrorismo, è la nostra nuova sfida». Si tratterebbe di un programma per ricostruire gli spostamenti dei soggetti che risultino positivi al COVID-19 mediante la geo-localizzazione. Oltre a questo, verrebbe verificato che i positivi non violino il periodo di isolamento a casa. Il procuratore generale avrebbe già dato la propria approvazione alle misure speciali, mentre i servizi segreti hanno garantito che non verrà violata la privacy e le informazioni non saranno sfruttare per imporre la quarantena, ma dovrebbero servire a ricostruire la mappa degli spostamenti degli infettati. Nonostante ciò deve evidenziarsi che la geolocalizzazione dei telefoni sembrerebbe possa garantire un livello di granularità abbastanza preciso nelle località urbane ed il fatto che questo venga presentato come uno

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

strumento di intelligence antiterrorismo suggerisce che si tratta di qualcosa di più di una semplice soluzione di base a livello di polizia, più di una semplice geofencing. Gdpr e direttiva ePrivacy A questo quadro internazionale si aggiungono le dichiarazioni di Andrea Jelinek, presidente del Comitato Europeo per la Protezione dei Dati (EDPB), secondo cui il GDPR fornisce le basi giuridiche per consentire ai datori di lavoro e alle autorità sanitarie pubbliche di trattare i dati personali nell'ambito di epidemie, senza la necessità di ottenere il consenso dell'interessato. Ciò vale ad esempio quando il trattamento dei dati personali è necessario per i datori di lavoro per motivi di interesse pubblico nel settore della salute pubblica o per proteggere interessi vitali (art. 6 e 9 del GDPR) o per adempiere ad altro obbligo legale. Per il trattamento dei dati relativi alle comunicazioni elettroniche, come ad esempio i dati relativi all'ubicazione ricavata da un dispositivo mobile, si applica la regolamentazione prevista dalle leggi nazionali di attuazione della direttiva ePrivacy che prevede il principio di giuridico secondo cui i dati relativi all'ubicazione possono essere utilizzati dall'operatore solo se resi anonimi, o con il consenso dei singoli. Le autorità pubbliche, specifica il presidente Jelinek, dovrebbero innanzitutto mirare al trattamento di dati relativi all'ubicazione in modo anonimo (cioè elaborando dati aggregati in modo che non possano essere invertiti ai dati personali). Ciò potrebbe consentire di generare rapporti sulla concentrazione di cellulari in un determinato luogo ("cartografia") - questo al fine di impedire assembramenti di soggetti. Quando non è possibile trattare solo dati anonimi, l'art. 15 della direttiva ePrivacy consente agli Stati membri di introdurre misure legislative che perseguono la sicurezza nazionale e, più in generale, la sicurezza pubblica. Questo tipo di legislazione di natura emergenziale, conclude, è possibile, secondo la regolamentazione europea, a condizione che costituisca una misura necessaria, appropriata e proporzionata all'interno di una società democratica. Conclusioni In conclusione, il modello garantista italiano ed europeo sembrerebbe limitare solo minimante il perimetro del diritto alla privacy riconosciuto ai cittadini, nonostante questa specifica emergenza si distingua da quelle passate per l'elevato livello di contagiosità del virus che dunque sembra potersi contenere solo mediante localizzazione e isolamento dei focolai, azioni prodromiche all'attuazione di adeguate misure di profilassi. Tutti gli altri modelli, invece, sembrano derogare al diritto alla privacy più significativamente, pur senza ricorrere al modello di sorveglianza di massa adottato in Cina. Il modello israeliano in primis, nel ricorrere a strumenti di intelligence, sembrerebbe sacrificare considerevolmente il diritto alla privacy, mentre in Usa e Sud-Corea le deroghe per fronte alla emergenza sanitaria sembrerebbero aver trovato nello strumento dell'app/sito un compromesso. Infatti, ricorrendo di fatto a una raccolta di dati attraverso siti/app si consentirebbe ai cittadini, seppur con minore capillarità, di conoscere basi giuridiche e scopo del trattamento un trattamento, attraverso informativa e condizioni d'uso, permettendo comunque al governo centrale la raccolta di dati sanitari e la mappatura in tempo reale dei dati necessari a far fronte all'emergenza.