I cinque pilastri dei diritti digitali nell'era del Covid-19

- Arturo Di Corinto, 26.03.2020

Hacker's Dictionary. C'è chi propone di usare app, siti e software per contenere il contagio, ma attenzione alle pratiche di raccolta dei dati che non servono né alla medicina né all'epidemiologia

Sappiamo tutti che in tempo di crisi i governi sono da sempre tentati di limitare le libertà fondamentali con azioni che aumentano la sorveglianza e minacciano la privacy. Perciò dovremmo anche sapere che al tempo del Coronavirus è importante seguire le direttive delle autorità sanitarie senza che venga meno il rispetto dei diritti umani e civili.

Di fronte alle molte proposte tecnologiche per contenere la pandemia, la Electronic Frontier Foundation ha realizzato una sorta di guida per la tutela dei dati basata su cinque parole chiave.

Proporzionalità: ogni limitazione della privacy deve essere necessaria e proporzionata. Qualsiasi programma che raccolga, in massa, informazioni identificabili sulle persone deve essere scientificamente giustificato e ritenuto necessario dagli esperti di sanità pubblica ai fini del contenimento del virus. Lo stesso vale per i Big Data.

Raccolta: deve essere fatta senza pregiudizi di nazionalità, etnia, religione, sulla base della reale possibilità di ognuno di contrarre il virus, come la storia dei suoi viaggi o la vicinanza con persone potenzialmente infette. E senza errori.

Scadenza: esiste il rischio che l'infrastruttura di sorveglianza dei dati che costruiamo per contenere Covid-19 possa sopravvivere a lungo alla crisi che si intendeva affrontare. Finita l'emergenza, vanno cancellati tutti i metodi invasivi creati per garantire la salute pubblica.

Trasparenza: qualsiasi uso governativo dei Big Data per tracciare la diffusione dei virus deve essere chiaramente e rapidamente spiegato al pubblico. Compresa la pubblicazione di informazioni dettagliate sui dati raccolti, il periodo di conservazione delle informazioni, gli strumenti utilizzati per elaborarli, i modi in cui questi strumenti guidano le decisioni sulla salute pubblica e se hanno avuto successo.

Contestazione: Se il governo cerca di limitare i diritti di una persona in base a questa sorveglianza dei Big Data l'interessato deve avere l'opportunità di contestarli tempestivamente.

La paura oggi offre grandi opportunità a chi vuole ridurre garanzie e diritti proponendo la sorveglianza biometrica, il monitoraggio dei social media o delle app sul telefono che non servono né alla medicina né all'epidemiologia.

Ad esempio in California le scuole già usano la tecnologia per spiare gli studenti a casa, a scuola e sui social grazie a software per la scansione dei post sui social media, telecamere con riconoscimento facciale e altre funzionalità utili a rilevare «comportamenti inappropriati». Persino monitorare la cronologia del browser e i messaggi inviati. In Cina usano dei caschi speciali per misurare l'attenzione degli studenti.

Stessi rischi per chi lavora. La piattaforma per videoconferenze Zoom consente agli amministratori di visualizzare dati dettagliati su come, quando e dove gli utenti si collegano.

Zoom fornisce anche un sistema di classificazione degli utenti e gli amministratori possono accedere ai contenuti delle call registrate, inclusi file video, audio, chat e trascrizioni, nonché ottenere dati di condivisione, analisi e gestione del cloud.

Chi usa Slack per il lavoro d'ufficio sappia invece che lazienda conserva i messaggi, che non possono essere eliminati automaticamente per tutto il tempo in cui l'area di lavoro esiste. Gli utenti gratuiti dell'area di lavoro hanno la possibilità di cercare tra i messaggi più recenti ma Slack, forze dell'ordine ed eventuali hacker possono vederli tutti.

Perciò, quale che sia lo scopo della raccolta e del trattamento, tutti i dati generati vanno protetti e tutelati da abusi. A beneficio di tutti.