La sorveglianza elettronica non è la risposta al Coronavirus

Hacker's Dictionary. Si moltiplicano le richieste di geolocalizzare i cittadini per limitare l'infezione. Ma si può fare solo nel rispetto della privacy e in un quadro di garanzie costituzionali

La gestione delle misure per arginare il Coronavirus ha rivelato la totale, marchiana e colpevole incapacità dei leader europei ed occidentali di preservare la salute pubblica. Macron lo sapeva dai primi di Gennaio, Johnson ha temporeggiato, Trump ha sottovalutato e la Merkel tentennato.

L'Italia ha fatto meglio. Tuttavia ritardi, errori nella comunicazione, notizie trapelate a giornalisti amici, impreparazione e indecisioni, hanno favorito la pandemia. Come

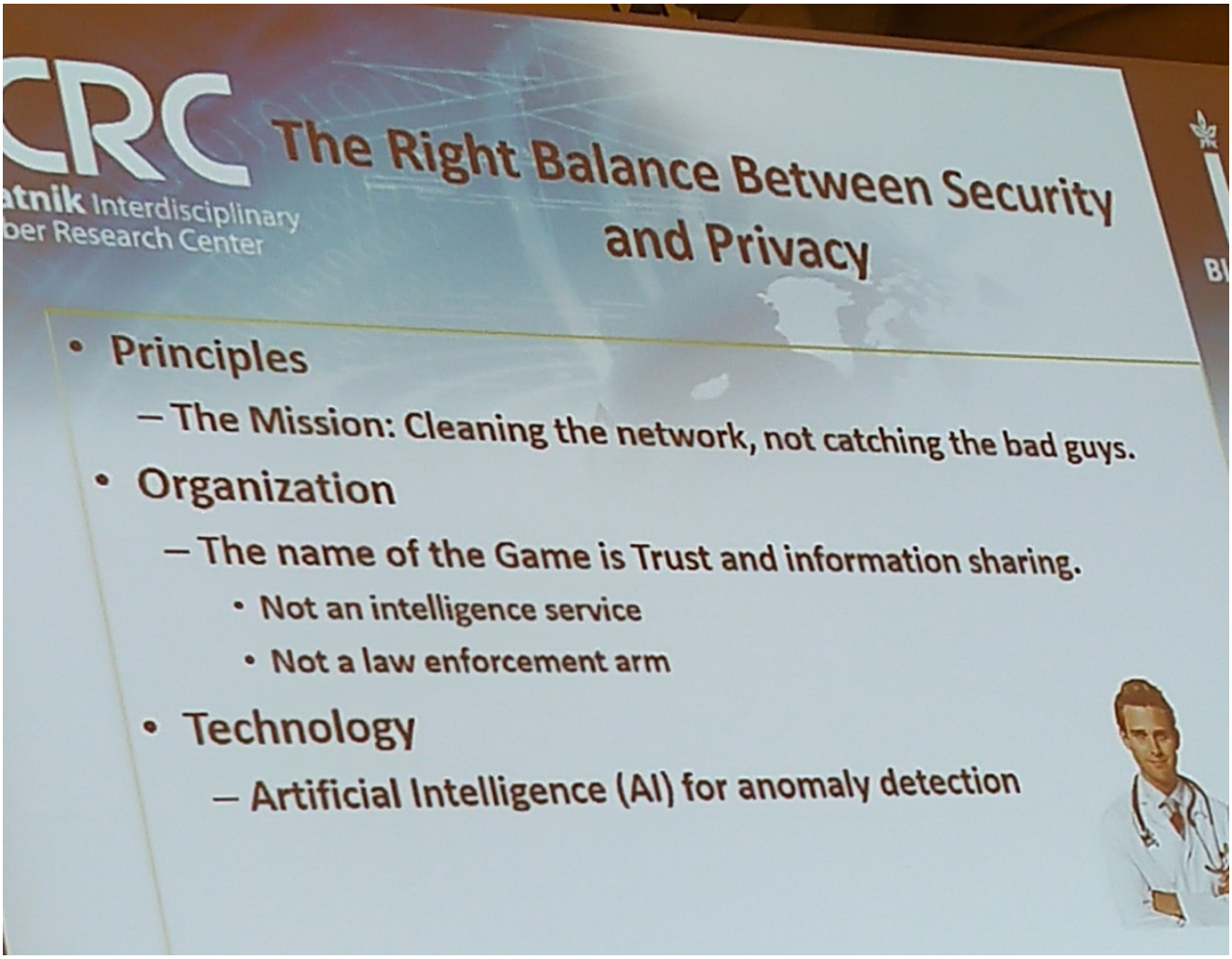
annunciare la zona rossa in Lombardia senza chiudere le stazioni.

Adesso si pensa di correre ai ripari utilizzando strumenti tecnologici di sorveglianza per tracciare gli spostamenti della popolazione.

L'unico leader "occidentale" capace di dirlo a chiare lettere è stato il capo ad interim del governo israeliano, Benjamin Netanyahu. Nel suo discorso alla nazione ha citato l'uso efficace dei dati telefonici a Taiwan per garantire la quarantena. Come pure è successo nell'autoritaria Singapore e nella Cina che prima aveva negato e poi censurato la notizia dell'epidemia.

Nethanyahu è stato molto criticato perché alludeva all'uso di sistemi di sorveglianza di tipo militare usati dall'antiterrorismo del suo paese e, pare, ai tool di una start up di nome Rayzone che usa Big Data, intercettazioni telefoniche, geolocalizzazione e fonti aperte – social network, social media e blog – per effettuare la sorveglianza elettronica del target.

Ora un approccio populista al problema chiede di decidere tra la salute e la privacy anche da noi. È una falsa dicotomia. I paesi democratici devono trovare un giusto equilibrio fra i due diritti fondamentali e preservarli entrambi.



Si potrà fare in Italia? Sappiamo che in caso di eventi eccezionali è possibile derogare dalla Gdpr, il regolamento europeo per la protezione dei dati personali. Ma a patto di capirne l'utilità.

Secondo il professore Michael Birnhack dell'università di Tel Aviv è possibile applicare un criterio proporzionale di sorveglianza per garantire privacy e salute pubblica. A cominciare dai target del Big Brother elettronico.

Per primi, i pazienti. Hanno bisogno delle migliori cure, la loro privacy è ridotta dall'ospedalizzazione ma protetta. La loro anamnesi dice tutto.

Secondo, le persone isolate in casa. Chi esce viola la legge. Dovrebbe essere un deterrente sufficiente per chi non ha motivi impellenti. Geolocalizzare quelli che consapevolmente violano le restrizioni potrebbe non servire perché

lascerebbero il telefono a casa.

Terzo, i malati di cui si vuole ricostruire il percorso dell'infezione. Non tutti ricordano dove sono stati prima di essere infettati. I dati del cellulare possono aiutare. Secondo il professor Birnhack la maggior parte delle persone è pronta a cedere quei dati e consentirne l'utilizzo. Rimarrebbero quelli che devono nascondere la frequentazione con pusher, amanti e prostitute.

Infine la localizzazione di chi è stato esposto a un paziente conclamato. Qui ogni informazione serve. Per avvisare quelli potenzialmente contagiati la sorveglianza telefonica può aiutare.

Si può fare con i dati delle compagnie telefoniche ma è una misura probabilmente sproporzionata. Secondo Birnhack si può fare il contrario: chiedere alle compagnie di contattare chi era nel posto sbagliato al momento sbagliato, offrendo una serie di garanzie legali.

Le possiamo immaginare: l'adeguata protezione cibernetica di quei dati; l'uso temporaneo e la distruzione degli stessi una volta utilizzati; il divieto di usarli per altri fini; un comitato di vigilanza sull'intero processo e il coinvolgimento del Garante della Privacy.