ISPI DOSSIER Maggio 2020

COVID-19: SORVEGLIANZA, PRIVACY E SICUREZZA CIBERNETICA

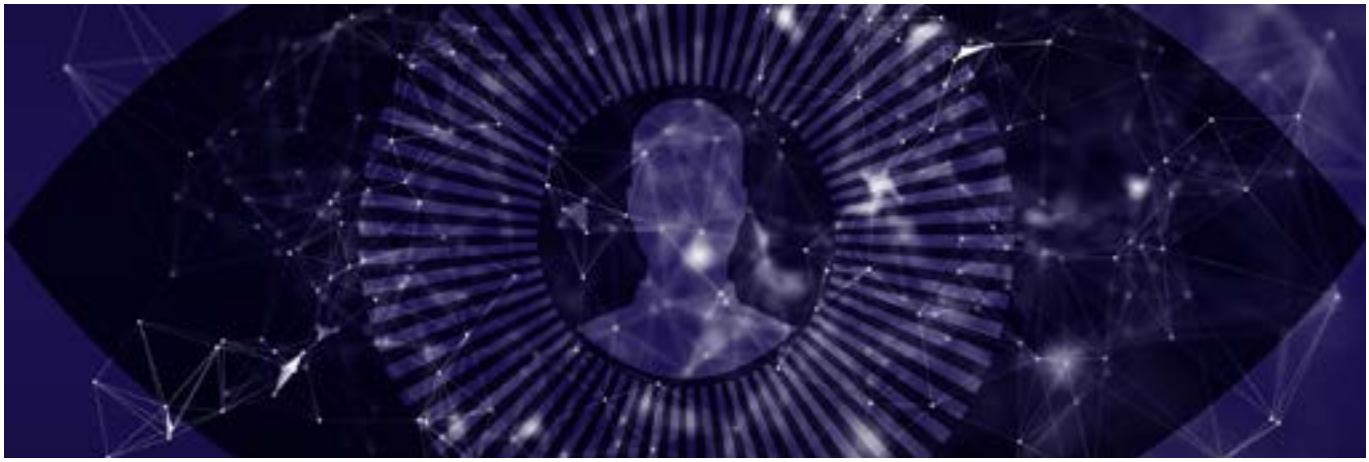
edited by **Samuele Dominioni, Fabio Rugge**

ISPI
ITALIAN INSTITUTE FOR INTERNATIONAL POLITICAL STUDIES

Maggio 2020

Stiamo vivendo la prima pandemia dell'era digitale. Ha colpito le nostre "nuove" vulnerabilità esponendoci, accanto ai rischi sanitari, alle crescenti minacce cibernetiche del mondo di oggi. La questione della cybersecurity delle piattaforme di tracciamento, della sorveglianza sanitaria, della sicurezza dei dati personali sanitari, sono solo alcuni dei temi sui quali si sta dibattendo molto in Italia e in molte altre parti del mondo. In gioco non c'è solo la lotta alla pandemia ma una sfida politica e securitaria cruciale per le nostre democrazie. Quali sono le implicazioni strategiche del contrasto tecnologico al Covid-19? Cosa è necessario fare affinché la tecnologia ci sia davvero d'aiuto? Quali sono i rischi di una "dipendenza" dal digitale nella lotta pandemia? E come si possono garantire privacy e diritti e allo stesso tempo la sicurezza cibernetica?

** Samuele Dominioni is a Research Fellow at the ISPI Centre on Cybersecurity, in partnership with Leonardo.*
** Counselor Fabio Rugge is Head of ISPI's Centre on Cybersecurity, in partnership with Leonardo.*



7. CONTACT TRACING: UN'APP PER OGNI PAESE?

Maria Sole Continiello (HSE)

ISPI
ITALIAN INSTITUTE FOR INTERNATIONAL POLITICAL STUDIES

Maggio 2020

Dominio cibernetico, sicurezza nazionale e valori nell'era Covid-19

Fabio Rugge
ISPI

La pandemia COVID-19 si sta rivelando un acceleratore di dinamiche e fenomeni latenti dinnanzi al quale gli attori pubblici (istituzioni, scuole, ospedali, case di riposo…), quelli privati (imprese, piccole medie e grandi) e i cittadini si son trovati in qualche misura impreparati. La prima pandemia dell'era digitale ha colpito le nostre "nuove" vulnerabilità, esponendoci, accanto ai primari rischi di natura sanitaria, alla minaccia cibernetica e a quella derivante dalla manipolazione delle informazioni. Ciò è accaduto simultaneamente in molti Paesi, rivelando fragilità a livello globale quanto a livello nazionale.

In questo contesto, il dominio cibernetico (per la sua intrinseca vulnerabilità, per la sua pervasività, per l'impunità ch'esso concede) si è confermato un terreno d'elezione per attività criminali e a varo titolo ostili – con effetti che vanno ben oltre il dominio dal quale promanano e finiscono per avere un diretto impatto sulla sicurezza nazionale. Ciò è probabilmente riconducibile a tre fondamentali ragioni.

In primo luogo, il confino impostoci dal COVID

Il Consigliere **Fabio Rugge** è Responsabile del Centre on Cybersecurity dell'ISPI, in collaborazione con Leonardo. Capo dell'Ufficio incaricato per la NATO e le questioni di sicurezza e politico-militari, Direzione generale per gli affari politici e la sicurezza, Ministero degli affari esteri e della cooperazione internazionale.

ha accresciuto la superficie d'attacco che esponiamo ad attori ostili: per continuare a lavorare ci colleghiamo di più alla rete, scambiamo più dati, e siamo dunque più esposti ai crimini informatici e alla penetrazione dei nostri sistemi da parte di altri attori malevoli. Siamo stati molto meno negli uffici, per le strade e nei negozi, e proprio per questo siamo sempre connessi, ed è quindi su internet che ci vengono a colpire.

In secondo luogo, ci affidiamo sempre di più al dominio cibernetico per la nostra resilienza economica (lo smart working, l'e-commerce, eccetera) e sociale (social networks, insegnamento a distanza, eccetera). Eventuali interruzioni di servizio dunque "costano", a noi personalmente ed alla nostra società complessivamente, più caro (come plasticamente dimostrano gli attacchi cibernetici ai danni degli ospedali) e, per converso, gli attacchi cibernetici divengono potenzialmente più vantaggiosi per chi li attua.

Infine, il dominio cibernetico ha ancora una volta dimostrato la sua intrinseca capacità di intervenire sui nostri processi cognitivi, di modellare la nostra comprensione del mondo, di consentire un'efficace manipolazione delle narrative e dunque di influenzare le nostre opinioni pubbliche. La cyber-enabled information warfare (ossia la guerra informativa fatta "su" e "grazie" al web) supporta la ricerca da parte di diversi attori di uno "status" internazionale, e dunque essa diventa un efficacissimo "braccio armato" del soft power (col quale ci si riferisce all'intrinseca attrattività del modello politico, sociale ed economico, ma anche alla manipolazione delle percezioni del target per rendere questo modello più appetibile). Ciò, peraltro, è vero anche rispetto alla minaccia eversiva di matrice interna: se la crisi economica innalzerà - come pure è possibile - il livello dello scontro sociale, è possibile che la dimensione digitale rappresenterà, anche qui, un palcoscenico privilegiato dello scontro. La sicurezza del dominio cibernetico si confermerà critica per lo sviluppo economico e per la stabilità sociale, oltre che per l'indipendenza e la salute dei nostri processi democratici. L'Internet of Things (IoT), lo sviluppo della capacità di computo ed i progressi nel campo dell'Artificial Intelligence (AI) stanno arrivando: siamo e saremo preparati a gestire l'impatto di questi acceleratori tecnologici?

Almeno inItalia, non siamo all'anno zero: le nostre strutture sanitarie (ed il personale che vi opera) hanno dato prova di straordinaria capacità, devozione e tenuta; il Governo da tempo mette in guardia e lavora per rafforzare gli strumenti normativi (golden power) ed operativi (Consob, Cdp, Sace, Banca d'Italia, …) a protezione della minaccia che può derivare da investimenti predatori (ossia legali, ma inopportuni) da parte di attori stranieri intenzionati a sfruttare il momento. Anche nel campo della sicurezza cibernetica, da anni lavoriamo attorno ad un'eccellente ed ancora attualissima strategia nazionale (il Quadro Strategico Nazionale per la sicurezza dello spazio cibernetico, del dicembre 2013) e tutti gli stakeholders - a partire dalla comunità intelligence e dalla Polizia Postale, ma anche nel settore privato, tanto sul lato dei "(cyber)security

provider" che su quello degli operatori che sono in prima linea nella difesa degli assetti nazionali più sensibili - sono da tempo impegnati per rafforzare la sicurezza e la resilienza nazionale, come peraltro dimostra il lavoro in corso per la messa in opera del c.d. "perimetro nazionale di sicurezza cibernetica". Se dunque da una parte sappiamo che la minaccia cibernetica è sempre più sofisticata, pervasiva e potenzialmente dirompente, dall'altra ci conforta sapere di poter contare su di un'architettura e capacità nazionali che, alla prova dei fatti, si stanno dimostrando all'altezza del compito.

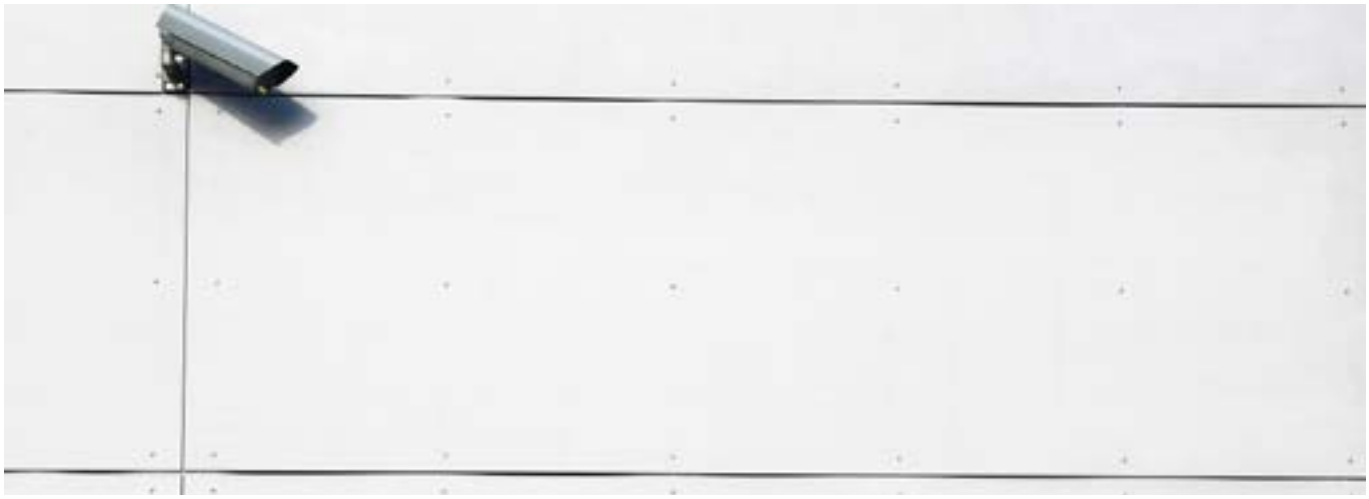
Se questa crisi sta facendo crescere un po' ovunque il tasso di digitalizzazione del Paese, matura inoltre – e questa è forse una delle poche cose buone che emergono dalla pandemia in corso – la comune consapevolezza di quanto la nostra prosperità, libertà e stabilità siano intimamente connesse alla sicurezza delle nostre reti. E siamo indotti forse a riconsiderare in chiave evolutiva (nell'era di Facebook, Twitter e Google) la sempre più anacronistica antinomia "privacy contro sicurezza". Ad ogni emergenza nazionale (sia essa idro-geologica, sanitaria o cibernetica) vediamo chiaramente come la sicurezza sia il bene propedeutico al godimento di ogni libertà. Se questa crisi ridefinirà almeno in parte il ruolo dello Stato (magari, per certi versi, invertendo l'ubriacatura iper-liberalista ed il progressivo depauperamento dello Stato centrale), forse si dovrà ripartire proprio dal concetto di sicurezza, e specie di "sicurezza partecipata" o (nella definizione offerta con straordinaria lungimiranza dal nostro legislatore con la legge di rifondazione della nostra comunità d'intelligence, la legge n. 124/2007) di "cultura della sicurezza". Questa più matura e diffusa consapevolezza è condizione necessaria per poter in futuro meglio mitigare e rispondere agli shock sistemici, ai "cigni neri" quale indubbiamente è questo COVID. Ne va della tutela e alla promozione dell'interesse nazionale – e in definitiva anche della nostra privacy individuale, quantomeno rispetto alle potenziali ingerenze di soggetti non nazionali.

Infine, vale forse la pena soffermarsi sul contesto internazionale in cui questa pandemia interviene: la crisi COVID è un acceleratore anche della Great Power Competition in corso. L'ambiente securitario diviene più volatile ed il confronto – anche nelle narrative nazionali – è sempre più aspro. Lo vediamo anche nel dibattito internazionale di queste settimane, troppo spesso "sopra le righe", e nei fenomeni globali che stanno emergendo e che in alcuni casi mai avremmo potuto nemmeno ipotizzate (il petrolio a costo negativo?). E ciò proprio mentre crescono le interdipendenze complesse (il c.d. entanglement, la compenetrazione, ad esempio, tra dimensione cibernetica, convenzionale e nucleare), e mentre il nostro orizzonte strategico diviene più imprevedibile, anche per via della progressiva erosione dei tradizionali strumenti multilaterali, tra cui quelli per il controllo degli armamenti. Great Power Competition significa che sempre più si profila a livello globale una competizione tra modelli alternativi ed una battaglia per vincere "hearts and minds", per imporre la propria narrativa. Ma attenzione, perché se Great Power Competition significa politiche nazionali egoistiche, "my country first", occorre considerare che esse trovano un limite intrinseco nella misura in

cui esse polarizzano lo scontro, proprio nel momento in cui più urgente è la necessità di coesione a livello nazionale e di forgiare e avvantaggiarsi di approcci condivisi a livello internazionale. La cybersecurity è questione primariamente culturale, ed è uno "sport di squadra". Credo sia dunque necessario ritrovare le ragioni valoriali di questi progetti comuni (anche infrastrutturali, si pensi al 5G), partendo dalle comunità di valori e dall'Alleanza a cui apparteniamo. Occorre, in altre parole, sviluppare approcci realmente condivisi, e rifuggire, anche in seno alle nostre alleanze più solide, visioni meramente transattive della nostra sicurezza. La radice valoriale è in ultima analisi il fondamento di ogni politica di sicurezza, inclusa quella per lo spazio cibernetico.

ISPI
ITALIAN INSTITUTE
FOR INTERNATIONAL
POLITICAL STUDIES

Maggio 2020



Covid-19: democrazia, tecnologia e fiducia

Samuele Dominioni
ISPI

La lotta mondiale alla pandemia di Covid-19 ha sicuramente avuto l'effetto di incrementare la presenza della tecnologia all'interno delle nostre vite. Dal lavoro da remoto ad una rinnovata socialità digitale fino all'utilizzo di piattaforme per l'intrattenimento o lo shopping. L'uso di servizi digitali è aumentato esponenzialmente. Allo stesso tempo, nel corso degli ultimi mesi, si è assistito ad un crescente dibattito rispetto a quelle che sono le potenzialità e le criticità della tecnologia per contribuire alla lotta contro la diffusione del coronavirus. Nel nostro paese si è dibattuto molto, sia a livello politico sia di opinione pubblica riguardo la piattaforma di tracciamento dei contagi. I pomi della discordia sono stati svariati, dalla procedura di selezione di "Immuni" alla composizione della Task Force, dalla scelta di quale protocollo utilizzare per lo sviluppo della piattaforma, a quale tipo di gestione del diario clinico del paziente.

Per quanto di natura domestica questi dibattiti si inquadrano all'interno di cornici ben più ampie. Innanzitutto essi hanno avuto il merito di porre

Samuele Dominioni è Research Fellow presso l'ISPI Center on Cybersecurity, in partnership con Leonardo. Ha conseguito un dottorato di ricerca in scienze politiche e storia politica presso l'Institut d'Etudes Politiques de Paris (Sciences Po) e presso la IMT School for Advanced Studies di Lucca,

l'accento su quello che è uno dei classici temi di filosofia politica: "sicurezza contro diritti" (incluso quello alla libertà e alla privacy). Intorno ad esso si risolve una questione fondamentale per l'equilibrio delle società democratiche liberali ma non solo. Inoltre, e qui la filosofia politica entra nel campo delle relazioni internazionali, la questione si inserisce nell'attuale Great Power Competition, in particolare dalla prospettiva della sfida tra democrazie liberali e regimi autoritari per quanto attiene a diversi indicatori di performance come quello della stabilità politica, della crescita economica e della digitalizzazione della società. La competizione ha già, e avrà sempre più, conseguenze mondiali anche alla luce della capacità di gestire la crisi economica e sociale che seguirà quella sanitaria. Le democrazie liberali, in quanto tali, devono garantire lo stato di diritto e l'equilibrio tra sicurezza e diritti è un esercizio continuo e non sempre facile. Infatti, questo equilibrio si deve adattare agli eventi e agli sviluppi della società contemporanea. Un caso relativamente recente è quanto avvenuto negli Stati Uniti con il Patriotic Act nel post 11 settembre 2001. I sostenitori del Patriotic Act rilevavano come la protezione della sopravvivenza stessa dell'ordine costituito necessitava una limitazione di alcune libertà e diritti individuali. Ovviamente, le implicazioni per la sospensione di questi diritti possono essere di varia natura ed essere, in misura variabile, sottoposte a scrutinio istituzionale e, infine, di breve o lungo termine. Di fronte alla crisi in corso, in cui un bene comune – la salute pubblica – è messo a repentaglio dalla diffusione di un agente patogeno, è necessario valutare soluzioni che preservino i principi fondamentali del nostro ordinamento, senza snaturarne il significato, e allo stesso tempo adottare politiche restrittive che garantiscano la sicurezza sanitaria del paese. Il rischio è di dare adito a normative liberticide che specialmente in regimi instabili possono determinare una deriva illiberale.

È necessario sottolineare che di fronte alla pandemia di Covid-19 i cittadini italiani, come quelli di quasi tutti gli altri paesi del mondo, hanno accettato, tutto sommato, di buon grado le misure restrittive ai movimenti e alle attività permesse. Il dibattito è piuttosto ruotato intorno all'utilizzo della tecnologia come fattore abilitante una maggior sorveglianza nell'ambito delle attività di contrasto al Covid-19. Vi sono due principali motivazioni alla base del clamore generato rispetto questa possibilità. Da un lato senza dubbio vi è stata la non lineare gestione del processo volto alla selezione della piattaforma Immuni e dei successivi passi per lo sviluppo della stessa. Dall'altro il rapporto tecnologia/libertà rimanda emozionalmente ad una atavica paura/eccitamento per la tecnologia, che si ritrova in molti prodotti culturali di natura distopica, a partire dal classico 1984 di George Orwell fino alle acclamate e popolari serie Black Mirror e Westworld. Le contrastanti emozioni generate da tali prodotti s'intersecano con l'angoscia generata dalle rivelazioni e dai moniti riguardo allo sviluppo di una sorveglianza di massa mondiale fatte in primo luogo da Edward Snowden.

Ad ogni modo, in un ordinamento democratico, per far sì che le soluzioni tecnologiche siano di un qualche effetto nell'estenuante lotta contro il Coronavirus, è necessario superare virtuosamente le preoccupazioni e le remore finora emerse e far sì che la app Immuni sia scaricata da quante più persone possibile. Infatti, come già evidenziato una copertura del 60% della popolazione è davvero difficile da raggiungere e pertanto serve innanzitutto coltivare la fiducia tra stato e cittadino. Una fiducia profonda e ben delineata da Marco Mayer nel suo articolo che si instaura innanzitutto tra il paziente e il medico per poi via via svilupparsi intorno al sistema stesso di sanità pubblica. Inoltre, per ottenere, incrementare e mantenere la fiducia è necessario, come ben spiegato da Stefano Mele, che nell'ideazione e nell'implementazione della piattaforma di tracciamento si osservino alcune imprescindibili e solidissime garanzie specialmente per quanto riguarda il trattamento dei dati degli utenti. Infatti, ciò che deve sorreggere la partecipazione in massa a questo processo di contact tracing è la necessaria convinzione di ciascuno rispetto l'utilità e la sicurezza della stessa (e quindi dei nostri dati), anche perché non vi sono soluzioni alternative eticamente sostenibili al suo uso volontario.

Vi sono tuttavia ancora dei punti sui quali è necessario fare chiarezza e auspicare delle soluzioni adeguate che vadano verso una maggior desiderabilità delle implicazioni socio-sanitarie che comporta la tracciabilità. Ad esempio, è necessario che una volta che l'utente riceva la notifica riguardo al suo possibile contagio (è entrato in contatto con qualcuno risultato positivo al Covid-19), quest'ultimo s'identifichi al servizio sanitario nazionale per seguire le predisposizioni del caso. Su questo punto, fondamentale per un corretto uso del tracciamento, si attendono ancora sviluppi normativi. Si può tuttavia ipotizzare delle soluzioni win-win per tutti, altrimenti si rischia di non ottenere i risultati sperati. In altre parole, come argomentato da Carlo Alberto Carnevale Maffé, è auspicabile pensare un nuovo patto sociale tra cittadino e Stato costruito sulla convinzione da parte di entrambi che il solo modo di combattere il virus è facendo squadra. L'idea è quella di favorire la diffusione e l'accettazione di uno standard sanitario su base volontaria, come quello della app Immuni, attraverso degli equi indennizzi. Non si tratta d'incentivi o disincentivi che hanno una natura contestabile e già esclusa dal governo; la logica è diversa e già utilizzata in altri settori secondo una giurisprudenza specifica (vedi ad esempio la sentenza della Corte Costituzionale 107/2012) volta a risarcire coloro impossibilitati a espletare le proprie attività perché in quarantena attraverso un contributo automatico di welfare.

È solo attraverso un aumento della fiducia verso le istituzioni, anche pensando un nuovo patto sociale tra cittadini e stato per l'occasione, che si può accrescere la volontarietà e quindi la partecipazione ai programmi di tracciabilità. Attualmente, è questa una delle sfide più importanti in cui è in gioco la credibilità delle democrazie liberali, in cui si deve preservare e proteggere la sicurezza e il corpus di diritti e libertà che ci contraddistinguono. Anche ai tempi del Covid-19.

ISPI
ITALIAN INSTITUTE
FOR INTERNATIONAL
POLITICAL STUDIES

Maggio 2020

Contact Tracing: appunti per una riflessione politica e di sicurezza nazionale

Stefano Mele
Carnelutti

L'emergenza sanitaria legata al Covid-19 sta da tempo dimostrando tutte le potenzialità tipiche di una pandemia globale di lunga durata, caratterizzata da un elevato tasso di mortalità e da un'altissima capacità d'impatto sul sistema sanitario dei paesi colpiti. Pertanto, nell'attesa di un vaccino, gli stati colpiti sono impegnati nella gestione di questa emergenza utilizzando una strategia tesa principalmente a contenere il diffondersi del virus e prevenire ulteriori contagi. La quasi totalità di essi, quindi, sta puntando da un lato sull'isolamento degli infetti e sulla loro decontaminazione, dall'altro sulla quarantena, sul distanziamento sociale, sulle scrupolose misure igieniche e – in un numero sempre maggiore di casi – anche sul tracciamento dei contatti sociali attraverso l'utilizzo delle tecnologie.

Tutti gli studi incentrati su quest'ultimo tema sono concordi nell'affermare che, dato il livello di contagiosità del Covid-19 e l'elevata percentuale di trasmissione attraverso individui pre- o a- sintomatici, il controllo dell'epidemia mediante il tracciamento manuale dei

Stefano Mele è avvocato, Partner di Carnelutti Studio Legale Associato, ove è il Responsabile del Dipartimento di Diritto delle Tecnologie, Privacy e Cybersecurity..

contatti sociali sia impossibile e quindi inutile. Contestualmente, però, questi stessi studi sono altrettanto concordi nell'evidenziare che l'utilizzo di una app per smartphone, capace di costruire un "ricordo" dei contatti di prossimità e di notificare immediatamente eventuali incontri con soggetti positivi, sarebbe utile per fermare l'epidemia solo se fosse utilizzata da un numero particolarmente elevato di cittadini e solo qualora fosse abbinata a politiche di rigido distanziamento sociale e a controlli sanitari a tappeto sulla popolazione alla ricerca dei contagiati (ad esempio, i tamponi). Occorre, quindi, delineare una strategia articolata su più piani di intervento, che parta dal riconoscimento quanto più immediato possibile della contagiosità del soggetto e arrivi al sistema di allerta attraverso l'app per smartphone. Non viceversa.

Peraltro, l'impiego di un simile strumento tecnologico solleva non pochi problemi etici e giuridici riguardanti – solo per citarne alcuni – l'accesso, la trasparenza, l'uso e la protezione dei dati personali dei cittadini, dei dati riguardanti il loro stato di salute, così come delle loro relazioni e interazioni sociali. Per di più, a poco possono servire processi tesi ad anonimizzare questi dati (e men che meno processi di "pseudonimizzazione"), in quanto la letteratura è piena di evidenze sul valore e l'utilità – anche commerciale – dei Big Data, così come sulla possibilità di de-anonimizzare i dati relativi alla mobilità dei cittadini, tracciare i loro dispositivi e acquisire informazioni (ad esempio, nel caso di utilizzo della tecnologia Bluetooth, tra i vari possibili, i cosiddetti 'Bluetooth Beacons').

Nonostante le numerose criticità, il governo italiano ha comunque deciso di utilizzare un sistema di allerta Covid-19 incentrato su un'app per smartphone che utilizza tecnologia Bluetooth, basando la propria decisione sulla legittima necessità di dover trovare in casi di gravissima emergenza – come quella odierna – un punto di equilibrio tra i diritti fondamentali della salute e della protezione dei dati personali, comprimendo in questo caso il secondo a favore del primo. Tuttavia, seppur legittimo, tale approccio necessita che il trattamento di questi dati debba obbligatoriamente sottostare ad alcune imprescindibili e solidissime garanzie, onde evitare che anche solo i rischi finora tratteggiati possano impattare in maniera evidente tanto sul piano politico, quanto su quello giuridico e della sicurezza nazionale.

In tal senso, quindi, il governo dovrà quantomeno provvedere a:

- Garantire che solo norme primarie possano incidere in maniera così profonda su un diritto fondamentale di libertà di tutti i cittadini italiani come quello alla protezione dei dati personali. Ciò, al fine di impedire che l'intero processo di creazione e gestione del sistema nazionale di allerta Covid-19 sia lasciato all'arbitrarietà di pochi e a semplici atti di natura amministrativa, sfuggendo così al confronto parlamentare e alle sue garanzie. Inoltre, tali norme primarie, che dovranno entrare in vigore prima dell'utilizzo dell'app di tracciamento da parte dei cittadini, dovranno avere come obiettivo quello di regolare complessivamente l'intero sistema nazionale di allerta Covid-19 (quindi,

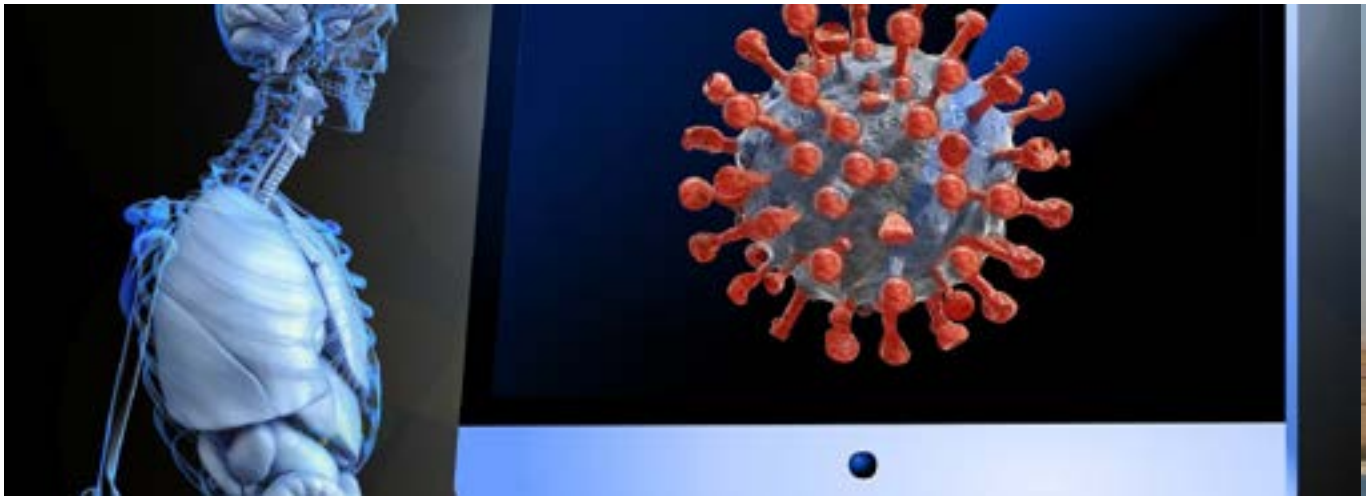
sia l'app che i sistemi informatici di raccolta dei dati e di allerta), le sue caratteristiche, il suo funzionamento, le misure poste a salvaguardia dei diritti dei cittadini, i criteri precisi in conseguenza dei quali un contatto con un soggetto giustifichi l'invio di un alert, così come le procedure che i cittadini dovranno seguire nel caso dovessero scoprire di essere entrati in contatto con un contagiato.
(Rischio che impatta sul piano politico e giuridico)

- Garantire la totale trasparenza nei confronti dei cittadini in ogni singola fase di vita del sistema nazionale di allerta Covid-19 (individuazione dell'esigenza e dei requisiti, realizzazione, protezione, implementazione e cessazione), esplicitando anche tutti i principi etici e normativi che guideranno questo percorso. Ciò, al fine di impedire che la mancanza di chiarezza in ciascuna delle fasi di questo processo possa dare adito a dubbi e strumentalizzazioni, soprattutto sul piano legale e dell'utilizzo dei dati personali, minando così la fiducia dei cittadini nell'uso finale dell'app per smartphone.
(Rischio che impatta sul piano politico)
- Verificare in maniera approfondita le relazioni, soprattutto economiche e di finanziamento, che la società aggiudicataria dello sviluppo dell'app per smartphone ha intrecciato nel tempo. Ciò, al fine di impedire che simili informazioni – rilevanti sia sul piano della qualità, sia su quello della quantità e soprattutto della capillarità – possano più o meno direttamente entrare nel possesso di attori europei e internazionali, sia pubblici sia privati, a vario titolo interessati.
(Rischio che impatta sul piano politico, giuridico e della sicurezza nazionale)
- Utilizzare solo sistemi informatici presenti all'interno del territorio italiano per erogare l'intero servizio, per conservare i dati dei cittadini e i loro backup, prevedendo anche che siano gestiti dal governo in maniera diretta ed esclusiva attraverso soggetti pubblici. Ciò, al fine di impedire che simili informazioni – rilevanti sul piano della qualità, della quantità e soprattutto della capillarità – possano più o meno direttamente entrare in possesso di attori europei e internazionali, sia pubblici che privati, interessati a vario titolo.
(Rischio che impatta sul piano politico, giuridico e della sicurezza nazionale)
- Verificare che nessun attore nazionale e soprattutto internazionale, ivi compresa la società aggiudicataria dello sviluppo dell'app per smartphone, possa in qualsivoglia modo accedere direttamente o incidentalmente ai dati raccolti, anche nel caso in cui questo soggetto abbia dato un qualsiasi apporto – anche tecnologico – per la realizzazione o per l'efficacia del sistema nazionale di allerta Covid-19. Ciò, al fine di impedire che simili informazioni – rilevanti sia sul piano della qualità, della quantità e soprattutto della capillarità – possano più o meno direttamente entrare in possesso di attori europei e internazionali, sia pubblici che privati, interessati a vario titolo.
(Rischio che impatta sul piano politico, giuridico e

della sicurezza nazionale)

- Rendere obbligatoriamente disponibile al pubblico il codice sorgente del software su cui si basa l'intera app per smartphone, permettendone l'audit da parte della comunità scientifica ed effettuando contestualmente anche dei penetration test sulla stessa, prima del suo massivo utilizzo da parte dei cittadini. Ciò, sia per una maggiore sicurezza dell'app per smartphone, sia per verificare che i dati dei cittadini non vengano mai trasferiti su altri server che non siano esclusivamente quelli pubblici deputati ad accoglierli.
  (Rischio che impatta sul piano politico, giuridico e della sicurezza nazionale)
- Applicare misure di sicurezza rigide e stringenti all'intero sistema nazionale di allerta Covid-19 (quindi, sia all'app che ai sistemi informatici di raccolta dei dati e di allerta), oltre che i principi di segregation of duty e need to know alle persone fisiche destinate a tutte le fasi di questo servizio. Ciò, al fine di impedire che simili informazioni – rilevanti sia sul piano della qualità, della quantità e soprattutto della capillarità – possano più o meno direttamente entrare nel possesso di attori europei e internazionali, sia pubblici che privati, a vario titolo interessati. Inoltre, soprattutto in questo caso, è importante ricordare anche come l'essere umano rappresenti sempre l'anello più debole della catena della sicurezza. Pertanto, controllare le persone fisiche che garantiranno questi servizi è altrettanto indispensabile quanto proteggerle dagli attacchi informatici esterni. Statisticamente, infatti, la metà di questi incidenti provengono dall'interno della struttura e sono causati, appunto, dagli individui per disattenzione e negligenza, ma anche – sempre più spesso – perché ricattati, costretti o pagati per ottenere le informazioni.
  (Rischio che impatta sul piano politico, giuridico e della sicurezza nazionale)

Solo l'accoglimento e la reale implementazione da parte del governo italiano di queste prime e imprescindibili garanzie potranno far sì che questo progetto incontri la fiducia dei cittadini, salvaguardando – pur nella necessità di risolvere quest'emergenza sanitaria – i loro diritti fondamentali e anche la sicurezza nazionale. Se ciò non dovesse avvenire, ci troveremmo dinanzi a un annunciato fallimento, colpevole peraltro di aver incredibilmente provato a barattare un diritto fondamentale di libertà dei cittadini, com'è quello alla protezione dei loro dati personali, con l'utilizzo di un'app per smartphone. Come se fossimo di fronte a un qualsiasi software commerciale e non a una delle possibili soluzioni utili a supportare la risoluzione dell'emergenza sanitaria più vasta di cui la nostra generazione ha memoria.



Non solo app: il nodo della digitalizzazione della sanità

Marco Mayer
ISPI

In questi giorni la rivista Tech del MIT mette in evidenza la vera e propria alluvione di app, dispositivi digitali e diavolerie tecnologiche spuntate da ogni parte per fronteggiare l'emergenza Coronavirus. Da una rapida rassegna si osserva che pochi progetti cercano di rispondere ad esigenze mediche specifiche o a ricerche epidemiologiche collegate all' andamento delle malattie infettive e in particolare alle lezioni apprese nel combattere Sars, Mers, Ebola, ecc. La grande maggioranza dei progetti di e-health non affronta alla radice temi sanitari irrisolti, ma si limita a puntare a una espansione quantitativa delle tecnologie digitali come se la loro diffusione fosse di per sé la panacea di tutti i mali. Non è la prima volta che accade. Nella loro fase iniziale più o meno in ogni settore i processi di digitalizzazione sono promossi e venduti come processi magici. A sette anni di distanza basta rileggere con occhio critico il celebre libro del fondatore di Google, Eric Schmit1 per capire quanto sia importante distinguere da un lato i valori aggiunti che caratterizzano l'era digitale, dall'altro le

Marco Mayer è professore a contratto al Master in cybersecurity presso l'Università LUISS Guido Carli di Roma, Ex consigliere speciale sulla sicurezza informatica del Ministro italiano degli Affari interni

promesse mancate e gli inconvenienti che essa comporta.

Per operare questa distinzione in ambito sanitario (da cui dipendono in buona misura la salute fisica e mentale, le malattie e nei casi più gravi la vita o la morte delle persone) conviene sgombrare subito il campo dai complessi risvolti di business che il diritto alla salute inevitabilmente si porta dietro. Le cartelle cliniche, i dati sui ricoveri, il consumo dei farmaci, le visite specialistiche, le campagne sui vaccini, per non parlare di aspetti più sofisticati (caratteristiche genetiche e profili psico-comportamentali dei pazienti) costituiscono gigantesche e preziose miniere di informazioni sia per i progressi della medicina, sia per il successo delle aziende private orientate al profitto.

Una vasta letteratura scientifica ha messo in rilievo da lungo tempo come la logica dell'economia di mercato non può essere meccanicamente trasposta nel comparto della sanità. Sul versante dei consumatori (i pazienti) un'intrinseca assimetria informativa limita fortemente il loro potere di scelta rispetto all'offerta (i medici). Sul piano della produzione di beni e servizi le legittime esigenze del profitto possono entrare in conflitto con necessità fondamentali per la medicina, ma non redditizie. Queste due peculiarità del comparto sanitario pongono un costante problema di bilanciamento tra logiche di mercato e imperativi della salute pubblica.

È in questa complessa cornice che occorre inquadrare il tema del tracing, attività cruciale – in assenza di vaccino – per sconfiggere le epidemie, Quando ad una persona viene diagnosticata la malattia infettiva (sia essa asintomatica o con sintomi più o meno gravi) è un preciso dovere degli operatori e del paziente fare il massimo sforzo per ricostruire i contatti personali, gli ambienti di lavoro e i luoghi frequentati nell'ultima settimana. Una volta conclusa questa mappatura di contatti è indispensabile informare le persone individuate perché esse possano sottoporsi nel più breve tempo possibile al tampone ed alla relativa analisi con i reagenti). Questa attività viene gestita con la dovuta discrezione da parte degli operatori sanitari con un giro di telefonate. È superfluo aggiungere che é un preciso dovere deontologico garantire a tutti i cittadini potenzialmente coinvolti l'assoluto anonimato.

Nel momento in cui – con l'avvio della fase 2 – alcuni milioni di lavoratori riaquistano la libertà di movimento la tempestività dei tamponi (e ovviamente delle analisi relative) diventa ancora più importante. Non basta più restare a casa, lavarsi le mani, indossare la mascherina e sanificare gli ambienti di lavoro; per contenere e possibilmente sconfiggere il Covid-19 occorre spengere sul nascere i focolai effettuando i tamponi alle moltissime persone a rischio già identificate a cui abbiamo fatto cenno in precedenza. Per svolgere questo compito assolutamente prioritario non c'è bisogno di un app; basta una comunicazione tecnologica elementare che già viene utilizata per le prenotazioni dei Cup. Per non escludere i molti anziani che non possiedono uno smartphone basterebbe inoltrare un sms a tutti gli interessati con la data, l'ora e il luogo dove fare i tamponi e le istruzioni relative.

I dati telefonici ci sono e i programmi di prenotazione anche, basta adattarli. Quando il commissario Domenico Arcuri ha dichiarato che tecnologie e mascherine sono indispensabili per attuare la fase due moltissime persone (in attesa da tempo) hanno pensato: "bene finalmente avremo a disposizione un sistema di prenotazione automatica dei tamponi; non resta che aspettare la convocazione via sms".

Purtroppo non è andata così. L'attenzione si è viceversa concentrata su altro, non sui gravi pericoli derivanti da possibili ritardi nell'effettuazione dei tamponi, ma sulla parola magica "App". In Italia da molte settimane la celebre "App Immuni" è sotto i riflettori dell'opinione pubblica e in questi giorni è addirittura oggetto di attenzione da parte del Copasir (Comitato Parlamentare di Controllo sull'operato dei nostri servizi segreti). Non sono assolutamente contrario ai processi di digitalizzazione della sanità, i vantaggi della telemedicina sono sotto gli occhi di tutti. Ma ancora una volta il punto centrale è come avviene il processo e chi lo gestisce. Immuni è partita con il piede sbagliato ed è inutile infierire. Ma ogni volta si ripete la stessa storia. Si dimentica che è indispensabile prima cambiare l'organizzazione e poi digitalizzare e non fare l'inverso. I medici, i dirigenti sanitari, il personale deve conoscere e sfruttare le opportunità offerte dalla rivoluzione digitale e tenerne conto nei progetti di riorganizzazione delle strutture. Gli informatici, gli esperti di AI e gli ingegneri delle telecomunicazione devono seguire la committenza della comunità medico-scientifica, del personale parasanitario e degli stessi pazienti e non viceversa. Le nuove tecnologie diagnostiche possono rimettere al centro il medico di base e le strutture territoriali con grandi vantaggi operativi e risparmio di costi.

Tuttavia guai a dimenticare che anche con le protesi tecnologiche più avanzate la fiducia tra medici e pazienti resta l'indicatore più importante per valutare il buon funzionamento di un sistema sanitario. La fiducia a cui faccio riferimento non é esclusivamente quella con il medico di famiglia, ma con l'insieme dei professionisti che i cittadini incontrano nel loro percorso di vita: il pediatra, il geriatra, il medico del pronto soccorso, il chirurgo, gli specialisti delle diverse discipline. L'unità di misura della fiducia non deriva da un fattore momentaneo, ma essa si sviluppa in un processo di interazione che i pazienti costruiscono in relazione al percorso diagnostico e terapeutico proposto dal medico e/o dei medici a cui si affidano oltre ovviamente al rispetto della riservatezza e agli altri loro doveri deontologici.

Questa fiducia alimenta in modo rilevante la reputazione tecnico-scientifica che circonda i professionisti nel territorio, negli studi specialistici, nei presidi ospedalieri e nelle cliniche universitarie. La fiducia (ragionata) è alla base della cooperazione attiva del paziente con il medico, di una buona organizzazione del sistema sanitario a livello territoriale/ ospedaliero e della partecipazione attiva dei cittadini alla tutela della salute pubblica. L'emergenza pandemia ha appena dimostrato quanto sia essenziale anche se non sufficiente. In altre parole se il cittadino si chiude in casa, o se rispetta la distanza fisica e indossa la mascherina quando esce blocca il contagio,

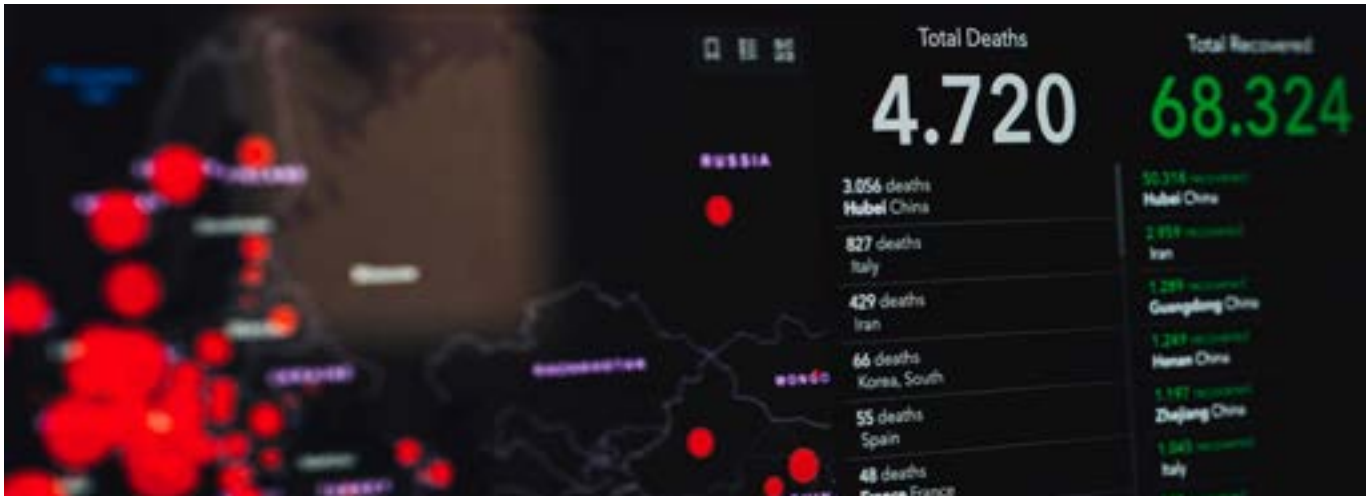
ma non sblocca il funzionamento della società. Troppe sono incognite: quanti sono i portatori sani? E quanti sono già impegnati nella fase 2. La verità è che risulta impossibile identificare i positivi asintomatici (e i casi lievi) finché il personale sanitario non attua i tamponi e le autorità sanitarie non procedono con le analisi nei laboratori disponendo dei reagenti necessari. Senza questo passaggio cruciale la curva sta scendendo, ma può risalire perché probabilmente sono troppo numerosi i cittadini non controllati che hanno permesso di muoversi. D'altra parte non si può stare fermi all'infinito e si rischia di finire in un circuito vizioso perché in assenza di dati sanitari viviamo nella nebbia. In questa cornice la fiducia si basa su quattro pilastri: A) distanza fisica; B) mascherine e igiene personale; C) tamponi; D) analisi e reagenti. Riguardo ai punti A) e B) i cittadini italiani sembra abbiano fatto il loro dovere, salvo pochissime eccezioni. Purtroppo sui punti C) e D) – salvo lodevoli eccezioni, ancora non ci siamo, né il Ministero della Sanità ha per ora indicato una deadline precisa in materia di tamponi.

Nel passato il medico condotto – al pari del farmacista e del maresciallo dei carabinieri - era una figura di riferimento – talora mitica – per intere comunità sociali con notevoli benefici sul piano dell'igiene pubblica. Negli ultimi decenni – con l'avvento delle nuove tecnologie diagnostiche – si é assistito viceversa a una "spersonalizzazione" della figura del medico di famiglia. In alcune situazioni inutile negarlo é stato erroneamente percepito come una mera figura "notarile": un compilatore delle ricette per diagnostica e farmaci. A ciò si collegano altri due fenomeni inquietanti – emersi con grande drammaticità in questi mesi di pandemia. Da un lato si registra l'assenza istituzionalizzata di un medico dedicato nelle RSA; per inciso le rette per gli assistiti sono peraltro pagate per il 50% dal sistema sanitario, ma esso é completamente estraneo alla loro gestione. Dall'altro in alcune realtà del nostro paese si assiste a una pianificazione del sistema sanitario centrato quasi esclusivamente sull'ospedale (pubblico o privato che sia) con un sostanziale abbandono della medicina territoriale. L'emergenza per il Covid-19 ha fatto emergere tali debolezze sistemiche. Ma al di là della pandemia, è indispensabile prepararsi a un cambiamento epocale che avverrà nel comparto sanitario con l'introduzione generalizzata di tecnologie digitali. Siamo alla vigilia di una gigantesca rivoluzione organizzativa che nel giro di pochi anni muterà completamente lo scenario. Attenzione, il miglioramento non è automatico, l'intelligenza artificiale è notoriamente stupida, saremo sempre più inondati da app di ogni genere. Chi è competente deve scegliere cosa serve davvero e cosa è superfluo per migliorare l'offerta sanitaria: solo così può guadagnarsi sul campo il bene più prezioso: la fiducia dei cittadini.

1. E. Schmit, La nuova era digitale: La sfida del futuro per cittadini, imprese e nazioni, Rizzoli, 2013

ISPI
ITALIAN INSTITUTE
FOR INTERNATIONAL
POLITICAL STUDIES

Maggio 2020



Oltre al coronavirus: i nostri dati sanitari sono sempre più appetibili

Pierluigi Paganini
CYBAZE

Mentre gli stati di tutto il mondo si confrontano con l'emergenza riguardante la pandemica COVID-19, il dibattito politico e pubblico è sempre più orientato alle problematiche di privacy e sicurezza proprie del settore sanitario.

Prima di entrare nel merito degli attacchi osservati dall'inizio della pandemia, cerchiamo di comprendere chi, e perché, è intenzionato ad accedere ai dati sanitari e per quale motivo le organizzazioni del settore sono particolarmente esposte ad attacchi cibernetici.

Purtroppo, il settore sanitario è da sempre un obiettivo privilegiato di gruppi dediti al crimine informatico. Secondo l'ultimo rapporto dell'associazione italiana di sicurezza CLUSIT il settore sanitario è tra quelli maggiormente interessati da attacchi informatici, addirittura è al terzo post nella graduatoria e presenta un trend in allarmante crescita (vedi Figura 1)

I principali responsabili di attacchi a organizzazioni che operano nel settore sanitario sono senza alcun dubbio gruppi di cyber

Pierluigi Paganini è Chief Technology Officer di Cybaze e membro dell'Agenzia dell'Unione Europea per la Cybersecurity.

criminali. Infatti, secondo i dati proposti dal CLUSIT, il 97%, degli attacchi è stato attribuito a gruppi dediti al crimine informatico, cyber criminali, mentre solo un 2% è associato a campagne di cyber-spionaggio e un 1% ad attacchi da parte di attivisti.

I dati sanitari sono merce preziosa nell'underground cyber criminale; talvolta il loro valore è superiore a quelle di informazioni finanziarie commercializzate in hacking forum. Infatti, i dati finanziari sono caratterizzati da una finestra temporale di utilizzo limitata; ad esempio, i dati associati ad una carta di credito devono essere utilizzati prima che la stessa sia bloccata dal proprietario accortosi di una possibile frode o prima che la stessa sia scaduta. Diversamente i dati sanitari di un individuo sono utilizzabili per attività criminali per tutto il tempo in cui è in vita un individuo e talvolta anche dopo la sua morte. I dati sanitari possono essere utilizzati per condurre molteplici attività illecite, quali attacchi di phishing, attacchi malware, e diversi tipi di frodi. Le cartelle cliniche possono essere molto redditizie per i criminali informatici, si pensi che il loro valore nel dark web varia dai $70 ai $150, in funzione di quanto siano dettagliate, di quale nazione provengano e della tipologia di paziente cui appartengano.

Di recente si è osservata un'allarmante tendenza, la disponibilità nei principali black market ed hacking forum di dati relativi ai medici stessi. Questi dati sono offerti nei principali mercati neri per circa US $500, gli archivi includono documenti assicurativi, diplomi e licenze mediche, ed autorizzazioni sanitarie di vario genere. L'utilizzo di queste informazioni potrebbe consentire ad un criminale di rubare l'identità di un medico e di operare in suo nome. Una tipica frode consiste nell'utilizzare l'identità di un medico per presentare richieste di risarcimento assicurativo fraudolente o ottenere prescrizioni per farmaci speciali, come gli oppioidi.

Accanto al furto di dati si registrano con estrema frequenza attacchi ransomware contro strutture ospedaliere, attacchi che spesso hanno portato alla paralisi di attività all'interno delle aziende colpite. In questo caso i criminali cercano di massimizzare il profitto richiedendo il pagamento di ingenti somme di danaro per consentire agli amministratori delle strutture di decifrare i dati criptati a seguito dell'attacco. Negli ultimi messi numerosi ospedali americani sono stati vittime di tali attacchi, e purtroppo anche durante l'emergenza COVID-19 si sono registrati episodi di tale natura nei confronti di ospedali in tutto il mondo, come ad esempio in Spagna e Repubblica Ceca.

Come già menzionato, anche gruppi mercenari, ovvero che operano per conto di governi, sono spesso dietro ad attacchi contro organizzazioni che operano nel settore sanitario per tre principali finalità: spionaggio, sabotaggio e auto-finanziamento attraverso crimini informatici.

Nel primo caso, gli hacker che operano per il governo sono alla ricerca di progetti, brevetti, risultati di sperimentazioni di farmaci o vaccini che potrebbero fornire allo stato per il quale operano un significativo vantaggio competitivo nel settore della ricerca. Di

Figura 1 – Fonte Rapporto Clusit 2020

VITTIME PER TIPOLOGIA	2014	2015	2016	2017	2018	2019	2019 su 2018	Trend
Gov - Mil - LEAs - Intel	213	223	220	179	252	203	-19.4%	↓
Multiple targets	-	-	49	222	304	395	29.9%	↑
Healthcare	32	36	73	80	159	186	17.0%	↑
Banking / Finance	50	64	105	117	156	141	-10.2%	↘
Online Services / Cloud	103	187	179	95	129	247	91.5%	↑
Research - Education	54	82	55	71	110	100	-8.3%	↘
Software / Hardware Vendor	44	55	56	68	109	83	-23.9%	↓
Entertainment / News	77	138	131	115	102	70	-31.4%	↓
Critical Infrastructures	13	33	38	40	57	37	-35.1%	↓
Hospitability	-	39	33	34	45	27	-40.0%	↓
GDO / Retail	20	17	29	24	39	50	28.2%	↑
Others	172	51	38	40	30	53	76.7%	↑
Org / ONG	47	46	13	8	18	18	0.0%	-
Gov. Contractors / Consulting	13	8	7	6	14	11	-21.4%	↓
Telco	18	18	14	13	11	17	54.5%	↑
Automotive	3	5	4	4	9	10	11.1%	↗
Security Industry	2	3	0	11	4	17	325.0%	↑
Religion	7	5	6	0	3	3	0.0%	-
Chemical / Medical	5	2	0	0	1	2	100.0%	↑
TOTALE	873	1012	1050	1127	1552	1670		

recente la Cybersecurity and Infrastructure Security Agency (CISA) e il National Cyber Security Centre (NCSC) del Regno Unito hanno annunciato di aver avviato investigazioni su attacchi contro università, organizzazioni di ricerca e società farmaceutiche. Secondo le agenzie gli attacchi sarebbero attribuibili a gruppi APT (Advanced Persistent Threat), ovvero attaccanti persistenti che operano per conto di governi stranieri.

Nel secondo scenario, quello di sabotaggio, gruppi di hacker che operano per governi stranieri conducono attacchi intenzionati a destabilizzare il contesto politico di un paese avversario. Efficaci quanto pericolose sono le campagne di disinformazione condotte su larga scala che hanno come obiettivo quello di delegittimare le politiche adottate dai governi per fronteggiare l'epidemia di COVID-19. L'agenzia europea European External Action Service ha recentemente pubblicato un rapporto che avverte di una "significativa campagna di disinformazione operata da attori di stato russi e che ha colpito gli Stati membri dell'UE". Secondo il Segretario di Stato Mike Pompeo, altri paesi stanno conducendo campagne di disinformazione, tra cui Cina e Iran. Queste operazioni potrebbe avere effetti destabilizzanti sulla popolazione, soprattutto in un momento critico come questo.

Infine, gruppi di hacker che operano per governi possono operare per sabotare le infrastrutture di un paese avversario oppure rubare informazioni e rivenderle nell'ecosistema criminale per auto-finanziare governi soggetti a sanzioni. In passato gruppi APT che operano per conto del governo della Corea del Nord si sono specializzati in attacchi contro le banche ed exchange di crypto-valute allo scopo di rubare fondi ed utilizzarli per finanziare attività militari del regime nonostante le sanzioni internazionali.

In un contesto come quello descritto è necessario uno sforzo congiunto di agenzie governative, forze dell'ordine, aziende di cyber security e le stesse aziende del settore sanitario per assicurare la loro protezione. Occorre che siano condivise informazioni sugli attacchi e sugli attori malevoli e che si implementino misure di sicurezza idonee ad incrementare la resilienza delle infrastrutture sanitarie

ISPI
ITALIAN INSTITUTE
FOR INTERNATIONAL
POLITICAL STUDIES

Maggio 2020

Dati sanitari: la necessaria evoluzione del diritto internazionale 2.0

Diego Bolchini
Università di Firenze

I più recenti eventi di cronaca cyber fanno sempre più riflettere su come porsi rispetto al fenomeno degli attacchi informatici alla luce di un sistema di diritto internazionale pubblico ed umanitario pensato per agenti umani e ancorato a criteri sovrani fisici. Le odierne vicende del cyber collidono in particolare con l'"ossessione" originaria del diritto internazionale per il territorio, essendo una disciplina interamente costruita sul concetto di spazio ed oggetti "tangibili".

Questa tangibilità fisica viene sempre più compressa ed erosa dalle nuove tecnologie, banche dati e piattaforme digitali. Si pensi, sul piano dei dati sanitari, ai c.d. "fascicoli sanitari elettronici" di user-pazienti e dei sottesi spazi di conoscibilità degli stessi. Quando si parla di sanità elettronica e di moderne tecnologie dell'informazione nella sanità si introduce de facto un livello "terzo" di tipo tecnico nella linea di rapporto fiduciario medico/paziente. Un livello che presenta ontologicamente - nella sua stessa natura tecnica - potenziali rischi per accessibilità, integrità e protezione dei dati

Diego Bolchini è docente di analisi delle informazioni per la sicurezza presso l'Università di Firenze - Corso di Perfezionamento Post-Laurea in Intelligence e Sicurezza Nazionale svolto in sinergia con la PcM e Research Associate Fellow presso l'Istituto Gino Germani di Scienze Sociali e Studi Strategici.

stessi rispetto ad attacchi cyber. Sono quindi evidenti le implicazioni strategiche della loro protezione cibernetica.

In senso più generale, non a caso, oggi il rapporto tra le nuove tecnologie e il diritto internazionale, comunitario e nazionale appare in pieno fermento e ri-adattamento simbiotico, aprendo diversi "coni di futuri" possibili. Un esempio ci viene fornito dal Manuale di Tallinn (Tallinn Manual on the International Law Applicable to Cyber Warfare) - pubblicato nel 2013 sotto la direzione del Prof. Michael Schmitt, United States Naval War College quale primo sforzo di codificazione di un diritto internazionale applicabile al cyber. In prospettiva, è lecito attendersi una continua evoluzione delle cyber operations anche al di fuori di conflitti armati dichiarati sul piano "reale" (che diviene oggi sempre più un mondo "legacy"). Difatti, lo stesso Manuale di Tallinn osserva come siano centrali gli effetti e non gli strumenti fisici utilizzati. Il caso emblematico, classicamente inteso, di operazione cibernetica, è rappresentato da un attacco informatico che faccia saltare la corrente elettrica in un ospedale, il che equivarrebbe (dal punto di vista dei soggetti e feriti ivi raccolti) a colpirlo fisicamente.

A tal proposito, si pensi agli effetti che un attacco alle infrastrutture sanitarie potrebbe avere ai tempi di lotta al Covid-19. Il contrasto alla pandemia ha incrementato esponenzialmente la superfice d'attacco anche per via di un ricorso crescente a piattaforme di tracciabilità. In tal senso, ulteriori problematiche potenzialmente impattanti sull'efficacia delle misure protettive potrebbero sorgere se si distruggessero o confondessero dati di tracking e contact tracing relativi all'epidemia di Covid-19. Da qui l'attenzione sul tema delle app anche da parte dell'organo di controllo parlamentare (COPASIR) previsto e istituto dalla Legge nr. 124 del 2007, per come emersa su diversi organi di stampa nazionali Al di là della tematica contingente delle app di tracciamento, sussistono ovviamente ulteriori categorie di dati oggi essenziali per la popolazione civile, come dati bancari o finanziari. Sono queste tutte dinamiche che si svolgono nello spazio cibernetico e che sempre più assumeranno rilievo nei rapporti internazionali così come nelle dinamiche sociali delle comunità e di singoli individui.

Un ampio spazio di dibattito sussiste per la questione relativa alla protezione, gestione, visibilità, oscuramento o distruzione di dati. Ci troviamo qui in una regione di frontiera, incentrata sulla manipolazione e la trattazione del dato in sé, laddove l'infrastruttura di rete che li trasporta rimane sullo sfondo. Fino a che punto allora i dati possono essere oggetto di attacco senza impunità? È di tutta evidenza che se si distruggono cartelle mediche digitali, con la conseguente impossibilità di ricostruire situazione terapeutiche, ciò può creare effetti concreti sugli individui.

I flussi e le associazioni di dati sono le nuove risorse da proteggere, essendo ormai fondamentali per la nostra società. Un nuovo sviluppo in termini di Opearational Law e di possibili precauzioni rispetto a potenziali interferenze digitali di attori malevoli va

quindi sempre più incoraggiato, se si pensa anche ai futuri scenari ipotizzati di Urban Warfare al 2035 e alla potenziale nascita di nuovi ambiti di rischio. Cosa potrebbe accadere con l'utilizzo di inedite armi cyber in mancanza di una chiara cornice epistemologica, giuridica, tecnologica e quindi operativa di riferimento? Come ci ricorda il Professor Luciano Floridi, docente di filosofia ed etica dell'informazione presso l'Università di Oxford, occorre "porsi le domande giuste al momento giusto" per avere risposte significative ed (auspicabilmente) corrette riguardo il nostro futuro.

ISPI
ITALIAN INSTITUTE
FOR INTERNATIONAL
POLITICAL STUDIES

Maggio 2020

Contact tracing: un'app per ogni paese?

Maria Sole Continiello
HSE

In molti paesi del mondo si sta scegliendo di utilizzare la tecnologia per sostenere gli sforzi nella lotta al Covid-19, in particolare per quanto concerne le piattaforme di tracciamento dei contagi. In mancanza di linee guida condivise e generali, ogni paese ha sviluppato un'interfaccia autonoma. Attualmente, 21 paesi hanno lanciato le loro contact tracing app e altri 11 le stanno sviluppando. Queste app permettono di individuare, e avvisare rapidamente, gli individui potenzialmente infetti, ricostruendo in via digitale la rete di contatti degli utenti. Pur se estremamente efficaci, l'utilizzo di queste app ha sollevato un acceso dibattito relativo al la tutela della privacy e la protezione dei dati degli utenti.

Le tecnologie di tracciabilità maggiormente utilizzate operano mediante tecnologia Bluetooth e ultrasuoni – tracciando le connessioni tra due telefoni a distanza ravvicinata – o attraverso sistemi di localizzazione GPS (Geo-tracking) che incrociando i dati dei percorsi degli utenti.

Maria Sole Continiello è una ricercatrice specializzata in Diritto Internazionale Umanitario e Diritti umani. Lecturer di International Human Rights Law e Post-Doctoral Research Fellow presso la Higher School of Economics di Mosca

In Asia, gli stati hanno prevalentemente utilizzato app di tracciamento basate sul geo-tracking GPS in sinergia con le più moderne tecnologie, quali: telecamere di sorveglianza integrate con sistemi di riconoscimento facciale, il tracciamento delle carte di credito e i braccialetti elettronici. Il governo cinese, in collaborazione con Alipay e Ant Financial, ha realizzato l'app Alipay Health Code che assegna ad ogni singolo cittadino un codice di diverso colore in base allo stato di salute, luogo di origine, spostamenti e contatti con persone possibilmente infette. L'app lanciata a Hangzhou è attualmente operativa in 100 città. Per quanto l'installazione dell'app sia volontaria, il QR code è obbligatorio per muoversi e accedere a luoghi pubblici e residenziali. L'app raccoglie tutte le informazioni condivise dall'utente sul browser, utilizza la posizione GPS e inoltra le informazioni raccolte dai dipartimenti governativi per tracciare e monitorare l'utente. Come prescritto dalla Cybersecurity Law del 2016 i dati sono criptati, anche se una volta processati possono essere condivisi con il sistema giudiziario e le agenzie governative e terze società o providers Non ci sono informazioni riguardo il limite temporale per la conservazione dei dati. La democratica Corea del Sud ha adottato l'11 febbraio l'app Corona100m. L'applicazione è volontaria, traccia mediante la localizzazione GPS gli spostamenti degli utenti, condivide i dati con il governo che avvisa gli utenti quando sono in prossimità di un luogo visitato da persone infette. Il sistema è centralizzato e lavora in sinergia con le telecamere di sorveglianza e il tracciamento delle carte di credito.

Il 21 marzo Singapore ha lanciato l'app Trace Togheter che si differenzia per un maggior rispetto della riservatezza dei dati degli utenti: l'app è volontaria, utilizza i sistemi Bluetooth, non ha accesso alla localizzazione né ai contatti dell'utente ed è open source. Tutti i dati sono conservati all'interno dei dispositivi per 21 giorni e sono criptati.

In Europa, già prima dell'inizio della cosiddetta "Fase 2", infuriava il dibattito sulla viabilità dell'utilizzo delle app di tracciabilità.
Sin dall'inizio di aprile, l'Unione Europea richiamava i suoi stati membri ad adottare una strategia comune che non consenta la cristallizzazione di sistemi di sorveglianza e targhetizzazione individuale. Le istituzioni da subito hanno ribadito la necessita di adottare misure di sicurezza forti a protezione dei dati, e il rispetto del GDPR e della Direttiva sulla e-Privacy. Queste dichiarazioni hanno trovato una positivizzazione nelle Toolbox adottate l'8 marzo dalla Commissione dove si ribadivano i principi di volontarietà dell'istallazione, richiesta di consenso per ogni funzionalità, anonimato (l'utente deve essere identificato attraverso un ID anonimo e temporaneo), crittografia dei dati e conservazione degli stessi su dispositivi individuali, ed infine temporaneità dell'utilizzo dei dati da parte delle autorità limitata al tempo necessario per combattere l'emergenza.
La Commissione indicava come idonea la tecnologia Bluetooth (sconsigliando la geolocalizzazione) e spingeva gli stati verso l'interoperabilità e l'utilizzo di un comune protocollo, prediligendo un sistema decentralizzato in base al quale i dati dell'utente sono conservati sui propri dispositivi (invece che in un database centrale).

Queste indicazioni non son state recepite da tutti i membri. La Finlandia, la Repubblica Ceca e Cipro hanno adottato app come SafePaths o Smart Quarantine basate sul geo-tracking. Una ulteriore spaccatura riguarda l'adozione dei diversi protocolli di conservazione dei dati. Infatti, la maggioranza degli stati (tra cui Germania, Italia, Irlanda, Austria e Svizzera) ad oggi prediligono un approccio decentralizzato (in base al quale i dati dell'utente sono conservati sui propri dispositivi invece che in un database centrale accessibile agli sviluppatori dell'app o ai dipartimenti e alle agenzie del governo) mentre la Francia è ancora incerta rimanendo ancorata al sistema PEPP-PT centralizzato, che lascia allo stato la competenza di analizzare i dati e avvisare gli utenti del possibile contagio. In modo simile, Regno Unito, Norvegia e Portogallo stanno valutando l'adozione di app per il controllo dei sintomi legate al sistema sanitario nazionale.

Gli Stati Uniti non hanno ancora adottato a livello nazionale una app di tracciamento, lasciando per il momento l'iniziativa agli stati federali e alle compagnie tech. Recentemente, il governo ha accolto con favore il progetto congiunto di Google e Apple che potrebbe esser adottatocome base per un app nazionale. A livello regionale, il Nord e il Sud Dakota stanno tracciando sinergicamente i dati GPS, WiFi, indirizzo IP, contatti del telefono e Bluetooth degli utenti al fine di risalire ai possibili contatti; mentre in Utah l'anonimato è protetto e la localizzazione degli utenti è vietata, rimanendo tuttavia centralizzata la gestione dei dati e in caso di necessita l'identificazione dell'utente da parte del personale sanitario.

A Mosca dalla fine di marzo è stato predisposto tramite decreto un rigido sistema di monitoraggio degli spostamenti di coloro che sono sottoposti a quarantena. Questo sistema si avvale delle celle telefoniche, delle telecamere di sorveglianza nelle metro e nelle aree pubbliche, del riconoscimento facciale e della geolocalizzazione GPS, nonché del monitoraggio dei social network e di altri dati. Con l'aggravarsi dell'emergenza e con il lockdown, molte città russe hanno attivato un sistema di QR code molto simile a quello cinese che viene rilasciato per ogni singolo spostamento e viene controllato mediante l'utilizzo sinergico delle tecnologie sopra citate.

L'app australiana COVIDSafe ha riscosso un incredibile successo con più di 3 milioni di download in pochi giorni. L'app è completamente volontaria, funziona tramite Bluetooth e segnala se si è venuti a contatto ravvicinato (meno di 1,5 m) e per più di 15 minuti con soggetti infetti. L'app permette al singolo di condividere con le autorità le informazioni che vengono registrate, crittografate dalla applicazione stessa, e conservate sui dispositivi per 21 giorni (secondo un sistema decentralizzato di raccolta).

Contrariamente a tutte le app precedenti, il download dell'app indiana Aarogya Setu è obbligatorio, in modo da raggiungere la totalità dell'utenza digitale. Lo stato impone pesanti sanzioni ai contravventori. Ufficialmente, la app traccia gli utenti attraverso localizzazione e Bluetooth, conservando i dati sul singolo dispositivo in forma crittografata, e

condividendoli in un secondo momento con il governo solo in caso di positività o di contatto con soggetti positivi.

In Israele, l'installazione dell'app Hamagen è volontaria. Questa utilizza i dati di localizzazione dell'utente, li confronta con le informazioni contenute nei server del ministero della Salute e rivela se ci siano stati contatti con persone positive negli ultimi 14 giorni. Se trova una corrispondenza positiva, l'app rimanda l'utente al sito del ministero della Salute, indicando le procedure da seguire e invitando l'utente a iscriversi. Tutte le informazioni rimangono nel dispositivo. Tuttavia al fine di rafaforzare i contolli anti-Covid 19il governo ha anche autorizzato lo Shin Bet ad adottare misure speciali di sorveglianza tecnologica (generalmente usate nella guerra al terrorismo) per monitorare i movimenti di tutti gli utenti tramite la localizzazione degli smartphone.

Il 29 aprile, il consorzio Google-Apple ha presentato una piattaforma di contact tracing che offre ai governi un set di definizioni e protocolli su cui impostare le diverse app di contact tracing nazionali, cosi da uniformare e permettere la interoperabilità delle applicazioni in tutti i paesi e per tutti i dispositivi. In una seconda fase, le due aziende mirano a offrire un sistema di tracciamento già integrato nei dispositivi, così da rendere superflue le diverse app, puntando sulla tecnologia Bluetooth low energy e sul sistema decentralizzato, sull'anonimato dei dati grazie all'uso di identificativi seriali e sul consenso dell'utente a condividere i proprii dati.

Questo nuovo protocollo infonde nuova speranza verso una pronta interoperabilità e uniformità nel mondo del tracciamento digitale che favorisca la trasparenza dell'algoritmo nel rispetto del principio di idoneità, di necessità e di temporaneità della misura di sorveglianza digitale adottata.