Ufficio stampa
e internet

Rassegna stampa tematica

Senato della Repubblica
XVII Legislatura

NOVEMBRE 2016
N. 36

TECNOLOGIE INFORMATICHE, PRIVACY E SICUREZZA

Selezione di articoli dal 15 gennaio al 22 novembre 2016

Sommario

Sommario

Sommario

la Repubblica

Data 15-01-2016
Pagina 25
Foglio 1

Il Grande Fratello in ufficio l'hi-tech spia la pausa caffè

Dal sensore che si accorge se la sedia è vuota al badge che misura lo stress Le nuove tecnologie riducono i confini della privacy sul posto di lavoro

GIULIANO ALUFFI

UN giornalista del *Daily Telegraph* ha trovato sotto alla scrivania, qualche giorno fa, una misteriosa scatoletta, troppo grande per essere una banale microspia. Tutti i suoi colleghi ne hanno trovato una simile. All'inizio, il parallelepipedo nero appariva enigmatico come il monolito di *2001 Odissea nello Spazio*. Un solo indizio visibile: la scritta OccupEye in rilievo. Una ricerca su Google ed ecco la verità che l'azienda stava celando: quegli strani aggeggi contenevano sensori di movimento e temperatura capaci di rivelare ai datori di lavoro se una scrivania è occupata. E quindi, di riflesso, se il titolare della scrivania sta lavorando o sta perdendo tempo, magari alla macchina del caffè. L'immediata sollevazione dei cronisti ha costretto la direzione del giornale prima a giustificazioni tardive — l'azienda avrebbe voluto monitorare l'uso delle scrivanie per risparmiare energia e riscaldamento spegnendo luci e caloriferi nelle stanze vuote — e poi a rimuovere le incolpevoli, ma non del tutto innocenti, scatolette nere.

> Il caso del *Telegraph* dove i cronisti hanno trovato una sorta di scatola nera sotto le scrivanie

Il controllo dell'email — purché aziendale e non privata — e della cronologia del browser del dipendente non è, oggi, una violazione della privacy: lo conferma anche una recentissima sentenza della Corte europea dei diritti dell'uomo, che ha respinto il ricorso di un cittadino romeno contro il licenziamento subito nel 2007 per uso personale, durante l'orario di lavoro, dell'account aziendale su Yahoo Messenger. Ma la scatoletta nera del *Telegraph* sembra segnare un cambio di paradigma. Il Grande Fratello non si limita a guardarci e a leggere ciò che scriviamo, ma si fa corporeo: vuole toccarci, annusarci, sentire il nostro battito cardiaco. O monitorare l'attività dei nostri neuroni: molti minatori e camionisti australiani indossano il cappellino SmartCap che, attraverso sensori simili a quelli dell'elettroencefalogramma, si accerta che siano vigili e reattivi. I magazzinieri dei supermercati Tesco indossano, in Inghilterra, un braccialetto che traccia i loro spostamenti e la percentuale di lavoro svolta: il dispositivo assegna punti se si finisce prima del previsto e penalità se si fa una pausa senza averla preannunciata. E in Messico si è appena spento l'eco della causa vinta dall'impiegata Myrna Arias contro l'azienda InterMex, che l'aveva obbligata a scaricare l'app Streetsmart di Xora: è un software che spiffera ai manager, grazie al Gps dello smartphone, gli spostamenti dei suoi sottoposti. «Mi fa sentire come un carcerato col suo braccialetto elettronico», si lamentò in tribunale la Arias. Parole che evocano il *Panopticon* digitale, un'evoluzione dell'idea avuta da Jeremy Bentham nel 1791: un sistema dove la mera possibilità tecnologica di essere sorvegliati basta a trasformarci in zelanti carcerieri di noi stessi.

«La cosa interessante, nel caso del *Telegraph*, è che l'intromissione nella privacy riguarda parametri puramente fisici — l'occupazione della scrivania — anche se il lavoro del giornalista è di tipo creativo: è paradossale che anche i frutti della *knowledge economy* vengano giudicati in base a indici come il calore corporeo» spiega a *Repubblica* il sociologo Will Davies, docente alla Goldsmiths University di Londra, che nel suo recente saggio *The Happiness Industry* (ed. Verso) ha analizzato i modi in cui le imprese misurano perfino realtà sfuggenti come la felicità del dipendente. «E c'è anche un altro messaggio, stavolta simbolico. Se le aziende non temono più di palesare il volto del Grande Fratello anche in ambienti che — come i giornali — creano opinione e possono facilmente denunciare un abuso, fin dove si potranno spingere? L'azzardo del *Daily Telegraph*, più che un oltraggio ai dipendenti, appare come un tentativo di sondare le acque.

LA STAMPA

Data 13-01-2016
Pagina 1
Foglio 1

STRASBURGO

Messaggi web
È lecito spiare
i dipendenti

Raphaël Zanotti

L'azienda non viola la privacy se spia i messaggi dei dipendenti

La Corte europea: si può licenziare se usano account di lavoro a fini privati

il caso
RAPHAËL ZANOTTI

La Corte dei diritti dell'uomo di Strasburgo ha appena confermato il licenziamento di un lavoratore che aveva usato l'account aziendale di Yahoo Messenger per comunicare con la fidanzata e il fratello durante l'orario di lavoro. Una sentenza che farà discutere in una società dove, sempre più spesso, la vita lavorativa interseca quella privata.

I fatti

Bogdan Mihai Barbulescu è un ingegnere romeno di 36 anni. Dal 2004 al 2007 è stato impiegato in una ditta di impianti di riscaldamento. Il 13 luglio 2007 riceve una comunicazione aziendale: «Dal 5 luglio a oggi il tuo account è stato monitorato». L'account è destinato a rispondere alle richieste dei clienti e l'azienda chiede conto a Bogdan dei suoi messaggi personali. L'ingegnere prova a negare e allora l'azienda gli invia 45 pagine di trascrizioni e lo licenzia. Che fare? Bogdan decide di portare in tribunale l'azienda sostenendo che il datore di lavoro non aveva diritto di leggere i suoi messaggi personali, alcuni di natura sessuale, e che sono state violate la segretezza della sua corrispondenza e la sua privacy. Perde, in tutti i gradi di giudizio. E allora Bogdan si rivolge alla Corte dei diritti dell'uomo, sostenendo che il suo Paese non gli garantisce le sue libertà fondamentali. È così? Secondo Strasburgo no. Il datore di lavoro, infatti, nell'aprire l'account gli aveva spiegato che doveva essere usato solo per lavoro. Inoltre, hanno accertato i giudici, il monitoraggio è avvenuto non su tutta la sua corrispondenza, ma per un breve lasso di tempo. Ed è diritto dell'azienda verificare l'adempimento contrattuale: Bogdan si era impegnato a usare quel tempo per lavorare e non per seguire le sue vicende private.

Il giudice dissidente

Detta così sembra semplice, ma non lo è. Non a caso uno dei giudici della corte non era d'accordo e ha voluto esprimere un parere diverso dai suoi colleghi. Secondo Pinto de Albuquerque, infatti, la sentenza non ha tenuto conto di alcuni aspetti fondamentali: 1) L'accesso a internet è ormai uno dei diritti umani e quindi il suo divieto tout court non è accettabile in un rapporto contrattuale; 2) La ricerca della massima produttività e redditività è un diritto dell'azienda, ma non può prevalere su quello della libertà di espressione; 3) Intercettare delle comunicazioni e raccogliere dati personali è una questione molto delicata, tanto che per un'intercettazione in campo penale è necessaria l'autorizzazione di un giudice. Possibile che per un provvedimento disciplinare questa cautela non sia prevista?

E in Italia?

«La sentenza di Strasburgo è in linea con altre emesse anche nel nostro Paese - dice Antonello Soro, il Garante della Privacy - L'aspetto fondamentale è la comunicazione aziendale: il lavoratore deve essere informato dei limiti di utilizzo degli strumenti aziendali, altrimenti nessun tipo di monitoraggio è possibile. Ma attenzione: anche in quel caso il controllo non è illimitato. Deve rispondere a principi di necessità e correttezza e deve avere finalità determinate, esplicite e legittime. Altrimenti diventerebbe un controllo massivo che violerebbe i diritti dei lavoratori». Questi principi sono stati elencati nelle Linee Guida espresse dal Garante nel 2007 e sono diventate ulteriormente importanti dopo che il Jobs Act ha modificato l'art. 4 dello Statuto dei Lavoratori. Proprio quello che vietava il controllo dei dipendenti.

la Repubblica

Data 23-01-2016
Pagina 18
Foglio 1

Il caso

PER SAPERNE DI PIÙ
ec.europa.eu
europe-v-facebook.org

Allarme sulla privacy "L'accordo con gli Usa deve essere rivisto"

Lo scontro dopo il ricorso alla Corte europea di un utente di Facebook

Il Garante in pressing sul governo italiano: "Fate presto" In ballo ci sono i dati personali e gli affari delle aziende

FRANCESCA DE BENEDETTI

I DATI degli europei in Usa non sono al sicuro e Safe Harbor, l'accordo che dal 2000 assicurava il passaggio di dati da Ue a Usa per Facebook, Google e molte altre aziende, non è più valido. Perciò urge un piano B. Sembrano tutti d'accordo, i difensori della privacy così come le aziende: la vacanza (legislativa) è durata troppo. L'ultimo allarme viene da Antonello Soro, garante italiano della privacy. Chiede al premier Matteo Renzi di fare pressing: «Le due sponde dell'oceano arrivino a una soluzione, basta incertezze». Interpellato da *Repubblica*, il governo risponde per voce di Sandro Gozi: «Confidiamo in un primo accordo di principio entro due settimane».

Il 6 ottobre la Corte di giustizia europea dichiarò non valido Safe Harbor. I giudici diedero ragione a Max Schrems, lo studente che aveva sollevato il caso: le informazioni personali in America non sono al sicuro, lo ha dimostrato Snowden. E senza tutele, i dati non possono viaggiare. Dal 6 ottobre il vecchio sistema non è più legale, ma il nuovo manca. Il garante è preoccupato: «Serve un accordo entro inizio febbraio, altrimenti si rischia il blocco. Ci sono 4500 imprese coinvolte: o agiscono fuori legge o si fermano. Immagina che crisi?». Gli dà sponda il presidente di Confindustria digitale Elio Catania: «Ha ragione Soro. Le aziende della Silicon Valley in qualche modo se la cavano, fanno i loro accordi e clausole contrattuali. Per le piccole e medie imprese invece è un calvario. L'incertezza ha un costo».

Dal gabinetto della commissaria Ue che sta negoziando con gli Usa, Vera Jourova, arriva una rassicurazione: «Lavoriamo a un quadro comune, siamo a stretto contatto con Washington con cui negoziamo intensamente da ottobre». Il garante europeo per la privacy Giovanni Buttarelli usa un cauto ottimismo. Da Bruxelles ricorda che «in tutte le negoziazioni importanti le vere soluzioni arrivano sul tavolo all'ultimo». Ma quando? E quali? «Qualcosa si muoverà verso fine gennaio. In ogni caso le authorities hanno dato inizio febbraio come limite massimo», ricorda Mister privacy Ue. Che prosegue: «Una soluzione che non tuteli la privacy rischia di essere di nuovo invalidata dalla Corte. È possibile allora che l'America estenda agli europei le garanzie già applicate ai cittadini Usa. Il Congresso ci sta lavorando». È questa per ora l'offerta messa sul piatto dalla segretaria al commercio Usa Penny Pritzker.

LE TAPPE

L'INTESA SAFE HARBOR
L'accordo Ue-Usa siglato nel 2000 consente di trasferire i dati personali dei cittadini europei nei server delle aziende Usa (come Facebook) presupponendo il rispetto della loro privacy negli Usa

LA SENTENZA UE
Dopo che lo NsaGate ha rivelato che la protezione dei dati personali negli Usa non viene garantita, il 6 ottobre 2015 la Corte di giustizia dell'Unione europea dichiara non valido il "Safe Harbor"

la Repubblica

Data 23-01-2016
Pagina 18
Foglio 1

IL PERSONAGGIO

"Non sprecate la mia battaglia per i diritti"

DA LUI tutto è cominciato. Max Schrems è lo studente di legge austriaco che ha sfidato i giganti della Silicon Valley. Ha messo nello zaino i dossier di Snowden: dimostravano che i dati degli europei, trasferiti in Usa, non sono protetti ma anzi sorvegliati. E ha chiesto all'Europa di difendere la sua privacy. La Corte di giustizia Ue gli ha dato ragione.

Schrems, lei ha vinto in tribunale. Ma poi la politica non ha trovato il piano B. L'Europa non fa abbastanza?

«Spero che la mia battaglia non vada sprecata. Ma chi accusa l'Ue di non aver agito a sufficienza sbaglia: l'Ue sta provando in ogni modo a trovare un accordo con gli Usa. Ma gli Stati Uniti non le vengono incontro».

Punta il dito sull'America?

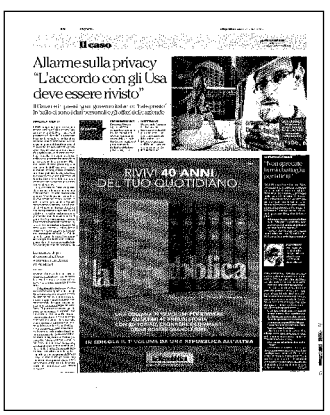
«Sì. Gli Usa devono fare un grande passo verso l'Europa, perché qualsiasi soluzione al ribasso rischia di essere di nuovo dichiarata invalida dalla Corte. Ma a me non risulta che Washington - dove mi trovo ora - stia facendo questi sforzi».

C'è l'ipotesi di una stretta di mano entro due settimane. E l'America potrebbe estendere le garanzie dei cittadini Usa anche a quelli Ue. Ne parla anche la segretaria al commercio Usa Pritzker.

«Se l'intenzione fosse quella, allora non basterebbero due settimane: una nuova legge in Usa richiede tempo».

Ma come soluzione è convincente?

«Per niente. I diritti di cui godono gli americani sono al ribasso rispetto ai nostri. L'Ue, in materia di tutela della privacy, è molto più avanti. Preferirei piuttosto il contrario: gli stessi diritti degli europei, anche per gli americani». *(f.d.b.)*


Il caso
Allarme sulla privacy
"L'accordo con gli Usa deve essere rivisto"
RIVIVI 40 ANNI DEL TUO QUOTIDIANO

Il Sole 24 ORE

Data 25-01-2016
Pagina 1
Foglio 1

Privacy, la Ue detta le regole per tutti

Rush finale per la riforma europea che accantona le normative nazionali

di **Antonello Cherchi**

Il codice della privacy ha i giorni contati. Così come tutte le altre normative nazionali sulla protezione dei dati personali. Sta per arrivare il regolamento della Ue che riscrive le regole per la tutela della riservatezza e che sarà immediatamente applicabile in tutti i Paesi membri. Manca solo il voto del plenum del Parlamento di Bruxelles, atteso per marzo. Dunque, regole uguali per tutti: dal diritto all'oblio alla portabilità dei dati all'introduzione della nuova figura del professionista della privacy.

Una novità che le aziende devono mettere in agenda per recuperare il ritardo: secondo una ricerca del Politecnico di Milano solo una grande impresa su cinque è al passo con l'information security.

Il 2016 sarà l'anno della privacy europea. Non che le regole che finora hanno disciplinato la riservatezza dei nostri dati personali non abbiano avuto una matrice comunitaria. Essendo, però, discese dalla direttiva 95/46, ogni Paese membro le ha poi declinate come meglio credeva. L'Italia le ha recepite nel 1996 con la legge 675 (quella che ha introdotto la cultura della privacy nel nostro Paese), poi riversate nel codice della riservatezza, il Dlgs 196/2003.

Regole che, così come quelle adottate nel resto dell'Unione, sono prossime alla pensione, perché la riforma della privacy in arrivo si compone di due provvedimenti: una direttiva, che interessa l'uso dei dati personali nell'ambito della sicurezza e delle attività di polizia e di giustizia e che avrà bisogno di essere recepita per diventare operativa nei vari Stati; un regolamento, che interesserà tutti i soggetti privati (persone fisiche e imprese) e parte di quelli pubblici e che sarà immediatamente applicabile. Non avrà, cioè, bisogno di alcun atto di recepimento, tranne un "interregno" di due anni concesso a ciascun Paese per adeguarsi alle nuove norme.

Questo vuol dire, in buona sostanza, che il codice della privacy italiano dovrà uscire di scena per far posto al regolamento. E così dovrà avvenire per le normative sulla riservatezza finora applicate nel resto dell'Unione. La strada scelta dalla Commissione europea nel 2012 - e prossima al traguardo con il voto definitivo del Parlamento europeo, che potrebbe arrivare a marzo, dopo un'articolata fase di confronto svoltasi negli ultimi due anni con il Consiglio Ue (si veda la scheda a fianco) - è quella di un provvedimento capace di garantire regole coerenti in tutta l'Unione, in grado di dare risposte uniformi alle nuove sfide, in particolare quelle imposte dalla tecnologia. L'utilizzo della Rete, il continuo sviluppo delle sue applicazioni, la globalizzazione dei dati e, dunque, il venir meno della nozione di territorialità, pretendono norme condivise, dall'Italia alla Francia, dal Portogallo alla Germania.

Il regolamento risponde a questa esigenza. Così come si presta meglio ad affrontare i problemi di circolazione dei dati posti dall'emergenza del terrorismo, per quanto questo sia un ambito in cui a dettare le regole - trattandosi di attività di intelligence - sarà anche la nuova direttiva.

L'Europa che si prepara a celebrare giovedì prossimo la giornata della privacy - appuntamento che si svolge a fine gennaio ormai da dieci anni - può, dunque, guardare a un imminente futuro costellato di importanti novità. Il regolamento contiene, infatti, una puntuale disciplina di ambiti finora rimasti ai margini delle normative nazionali sulla privacy. Per esempio, il diritto all'oblio, cioè a essere "dimenticati" da internet, riconosciuto dai giudici della Corte Ue nella primavera del 2014 con una sentenza che ha imposto a Google di rimuovere le informazioni personali vecchie e non aggiornate (e sempre che non abbiano un interesse pubblico). Oppure, il diritto alla portabilità dei dati: il regolamento riconosce la possibilità al cittadino di chiedere - per esempio a un'azienda - l'elenco delle informazioni personali che lo riguardano e di trasferire quei dati a un'altra impresa.

Altra novità in arrivo è la necessità per chi gestisce le informazioni personali di effettuare una valutazione dell'impatto che l'utilizzo dei dati può avere, in particolare quando si verificano condizioni che possono presentare un rischio significativo per i diritti e la libertà della persona.

Si prevede, inoltre, un potenziamento dell'informativa (la comunicazione che chi gestisce i dati personali deve fornire nel momento della raccolta delle informazioni), con la possibilità di rendere la procedura più familiare attraverso il ricorso a disegni, icone o altre forme grafiche.

C'è, poi, l'introduzione del Data protection officer (Dpo), un professionista che deve controllare e coordinare l'attività di quanti - all'interno di un'azienda o di un ufficio pubblico - utilizzano i dati personali. Si tratta di una figura già prevista da alcune legislazioni europee e che il regolamento estende a tutti i Paesi, imponendola alle pubbliche amministrazioni e a quelle imprese in cui il trattamento delle informazioni personali presenta profili di particolare rischio.

Infine, il regolamento ridisegna compiti e poteri delle Autorità nazionali, chiedendo - in linea con l'uniformità delle nuove regole - maggiore cooperazione.

Il Sole 24 ORE

Data 25-01-2016
Pagina 9
Foglio 1

Sicurezza informatica. I dati del primo Osservatorio del Politecnico

Tra le grandi società solo il 20% è ben difeso

di **Enrico Netti**

Solo una grande azienda italiana su cinque può considerarsi ben strutturata sul fronte sempre più caldo dell'information security. La metà sta invece muovendo i primi passi di un percorso organico, mentre il restante 30% è consapevole del problema, ma tentenna nell'attuare piani concreti. A tracciare il quadro è la prima edizione dell'Osservatorio Information security & privacy del Politecnico di Milano, che verrà presentato venerdì a Milano.

Sul versante degli investimenti per la protezione dei dati e di altri asset intangibili delle imprese si registra un aumento medio della spesa del 7% e tra i *big spender* spiccano le società dell'area media, tlc e finanza, che incrementano i loro budget. Fanalino di coda, le imprese del manifatturiero (solo una su tre punta ad aumentare le risorse), mentre il retail è stabile. «Tra le imprese è scarsa la tendenza ad affrontare in modo sistematico i temi sicurezza e privacy, mettendo a disposizione le risorse necessarie solo sotto la spinta degli obblighi di legge - osserva Gabriele Faggioli, responsabile scientifico dell'Osservatorio e presidente Clusit -. Certo, aumenta il timore di attacchi "interni" all'azienda e cresce il peso dei dispositivi mobili, fattore rilevante di rischio».

Che i rischi siano in aumento lo confermano le cronache del 2015: dagli attacchi con il ransomware Cryptolocker (i computer si bloccano fino a quando non viene pagato il "riscatto") alle violazioni subite (saccheggio di dati top secret) dalla Hacking Team, multinazionale che fornisce servizi di intrusione offensiva e sorveglianza a governi e servizi segreti di tutto il mondo.

Secondo la ricerca del Politecnico, gli attacchi informatici sono la principale minaccia per quasi due imprese su tre e gli hacktivist in un caso su due, ma tra i rischi spiccano anche i dipendenti interni (49%) e i consulenti aziendali (30%). Nel campionario degli incidenti affrontati negli ultimi due anni c'è un mix tra malware (80%), phishing (70%), spam (58%), attacchi ransomware (37%) e frodi (37%). Tra le cause si segnalano la violazione delle policy aziendali, la distrazione, l'accesso con smartphone e tablet ai dati aziendali. «Devono essere definiti i ruoli di responsabilità per attuare strategie di It security - spiega Alessandro Piva, direttore dell'Osservatorio information security & privacy del Politecnico di Milano -, pianificando ruoli e responsabilità manageriali». Oggi solo in quattro grandi aziende su dieci è presente il responsabile della sicurezza.

Nel campione osservato una società su tre ammette di avere subìto nel 2015 il furto di dati: molto spesso erano dati operativi interni, informazioni *price sensitive*, sui clienti o sui pagamenti, ma anche elementi di proprietà intellettuale, dati relativi a gare, informazioni di mercato e sui competitor. Con pesanti danni in termini reputazionali.

Per quanto riguarda la privacy, nonostante l'attività del Garante, secondo l'Osservatorio ci sono molti freni: dalla difficoltà nell'identificare le migliori metodologie (60%) alla scarsa attenzione del top management (38%), dai ruoli di governance (23%) alla scarsità di competenze (25%).

«Ai *cloud provider* viene richiesto di dichiarare le misure di sicurezza a difesa dei contenuti - conclude Faggioli -. Serve uno sforzo di trasparenza e di tutela contrattuale e normativa non ancora soddisfacente».

enrico.netti@ilsole24ore.com

I NUMERI

+30%

Cybercrime

Nel primo semestre 2015, secondo i dati Clusit, gli attacchi informatici gravi hanno segnato un aumento di circa il 30% rispetto al periodo luglio-dicembre 2014

+7%

Il budget

Nell'ultimo anno sono aumentate le risorse delle grandi imprese per proteggere dati e infrastrutture Ict: a investire di più sono le società dei settori media, tlc e finanza, seguite da Pa, sanità e utility

21%

Informazioni sensibili

In caso di violazione dei sistemi vengono perlopiù rubate informazioni operative interne, dati price sensitive e sui clienti (in un caso su cinque), credenziali di accesso e informazioni sulla proprietà intellettuale, oltre a documenti relativi ad attività commerciali


Tutela dei dati

Privacy, la Ue detta le regole per tutti

Tra le grandi società solo il 20% è ben difeso

LA STAMPA

Data 03-02-2016
Pagina 26
Foglio 1

OBBLIGHI PIÙ SEVERI PER LE AZIENDE CHE IMMAGAZZINANO INDIRIZZI, RIFERIMENTI E CARTE DI CREDITO

Privacy, c'è l'accordo Usa-Ue "Più garanzie a chi usa il web"

Stretta contro gli abusi dei colossi americani sui dati degli utenti

MARCO ZATTERIN
CORRISPONDENTE DA BRUXELLES

Obblighi di tutela stringenti per tutte le società americane che maneggiano i dati personali dei cittadini europei, più potere alle autorità della privacy nel Vecchio Continente, ma anche un impegno scritto del Dipartimento di Stato sul fatto che l'Intelligence a stelle e strisce non abuserà dei nostri dati, e un difensore civico «made in Usa» a cui si potrà ricorrere in caso di violazioni sospette o manifeste. Ecco il nuovo «Safe Harbor» che gli sherpa di Bruxelles e Washington hanno disegnato per colmare il vuoto creato in ottobre dalla Corte di Giustizia Ue, che ha invalidato la struttura varata nel 2000 per salvaguardare chi lavora, compra e comunica su Internet. Ha quattro pilastri e potrà entrare in vigore presto. A patto che nessuno abbia nulla da ridire.

Un sollievo per Amazon

Le imprese che animano il business sulla grande rete tirano un sospiro di sollievo. Amazon, Ebay e le loro sorelle possono interrompere la frenetica attività con cui s'erano messe a studiare vie alternative per assicurare il rispetto della vita privata e osservare le norme europee, condizione necessaria per rimane sul mercato. Le regole Ue per la protezione dei dati impediscono infatti il trasferimento dei dati dei cittadini senza che vi sia la garanzia d'una protezione adeguata nel rispetto delle regole della privacy. Quindici anni fa per questo era nato il «porto sicuro» in cui quattromila imprese americane avevano autocertificato che le informazioni di clienti e iscritti erano trattate secondo la legge.

L'escalation nei rapporti

Poi le cose sono cambiate. Le inchieste seguite alle rivelazioni del «whistleblower» Edward Snowden hanno diffuso a fine 2013 un sostanziale senso di incertezza nell'opinione pubblica europea a proposito dell'affidabilità della tutela oltreoceano. In ottobre, la Corte di Giustizia Ue ha messo la ciliegina su una torta che stava lentamente andando a male e che, su base bilaterale, si provava da mesi a cucinare daccapo. La massima magistratura di Strasburgo rispondeva a un ricorso di un privato cittadino austriaco, Max Schrems, e decretava l'invalidità dell'Harbor. Di fatto, la delibera sospendeva la struttura per la protezione dei dati e avviava un nuovo negoziato per ristabilirla. La deadline era il 31 gennaio. L'intesa è arrivata ieri.

L'accordo preliminare, approvato dalla Commissione Ue, impone alle società americane che desiderano importare dati personali dall'Europa di votarsi a un insieme consistente di procedure su come elaborare e immagazzinare indirizzi, numeri di carte di crediti, riferimenti anagrafici, scelte di consumo e così via. Il loro comportamento sarà monitorato dal Dipartimento del Commercio, ma anche impugnabile delle autorità europee per la privacy. Washington ha accettato di limitare al massimo il margine di azione dei servizi segreti, a partire dalla Nsa, definita «invasiva» dalla Corte Ue. Inoltre, ha escluso qualsiasi pratica di «sorveglianza di massa», cosa che del resto si era verificato in passato.

Possibilità di ricorsi

La novità più importante è però la possibilità di ricorso. Le società stesse avranno obbligo di risposta rapida. In caso contrario, un meccanismo di contenzioso sarà accessibile gratuitamente. Per i reclami sulle infrazioni delle autorità di Intelligence, sarà creato un apposito Ombudsman. L'incognita è che l'accordo si riferisce solo ai principi e i dettagli richiederanno ulteriori trattative, nota Inno Genna, analista bruxellese del settore comunicazioni. E «il rischio che la cornice possa essere considerata insufficiente resta presente».

Il Sole 24 ORE

Data 03-02-2016
Pagina 1
Foglio 1

L'ACCORDO SAFE HARBOUR FA FELICI ANCHE LE AZIENDE USA

Patto sui dati, successo europeo e della privacy

di **Luca De Biase**

Era un labirinto normativo che rischiava di imbrigliare il traffico online. E ieri ha trovato una soluzione. L'accordo "Safe Harbour", dal 2000, regolava la circolazione dei dati tra le due sponde dell'Atlantico: i governi degli Usa e dell'Europa si fidavano reciprocamente sul rispetto dei diritti dei cittadini. Ma Edward Snowden aveva dimostrato che l'agenzia Nsa praticava la sorveglianza di massa sugli utenti della rete, infischiandosene della privacy. E lo scorso ottobre la Corte Ue ha deciso di dichiarare illegale l'accordo del 2000. Ebbene: ieri la Commissione europea e il governo americano hanno annunciato un nuovo accordo. Che impegna gli Usa a non fare sorveglianza di massa sugli europei. È una vittoria dei diritti umani. E soprattutto delle aziende americane.

Il puzzle disegnato dalla fine del Safe Harbour era quasi insolubile. Il caso della Microsoft era emblematico. La decisione della Corte Ue impediva di fatto all'azienda americana di consentire l'accesso delle autorità Usa ai dati europei. Ma sulla base delle leggi americane, un tribunale di New York pretendeva di poter vedere i dati di utenti dei servizi di mail dell'azienda di Redmond registrati su computer che si trovavano i Europa. E quindi la Microsoft non poteva essere in regola contemporaneamente in Europa e negli Usa.

Il vuoto normativo seguito alla fine del Safe Harbour rischiava di bloccare lo sviluppo delle transazioni online: le prenotazioni di alberghi, le ricerche di pagine web, le chiacchiere sui social network, i pagamenti transatlantici, e mille altre attività potevano essere fermate dall'incertezza sulle norme che regolavano il trattamento dei dati personali.

I principi europei, basati sulla tutela dei diritti della persona, si scontravano direttamente con i principi americani, basati sulla libertà di espressione e di circolazione delle informazioni. Una soluzione andava trovata. E quella uscita dalle negoziazioni dei mesi scorsi appare come l'accettazione americana del punto di vista europeo.

Una novità. Dovuta essenzialmente all'opera di lobby svolta dalle aziende americane preoccupate di perdere il contatto con il gigantesco mercato europeo, dopo le rivelazioni di Edward Snowden sulla sorveglianza di massa praticata dall'Nsa.

Google e le altre compagnie internet avevano preso decisamente posizione. La Microsoft aveva persino avviato un programma di costruzione di datacenter nel Regno Unito, in Olanda, in Germania che, dichiarava, avrebbero seguito le leggi europee e avrebbero ridotto la necessità di far transitare i dati da una parte all'altra dell'Atlantico. In Germania, addirittura, avrebbe posto i suoi datacenter sotto la tutela fiduciaria della Deutsche Telekom, in modo da proteggerli dalle pretese americane. La Microsoft insomma aveva scelto. E aveva trovato un modo per proteggere la relazione di fiducia con i suoi utenti europei.

Pragmaticamente le autorità americane hanno fatto marcia indietro. Si impegnano a non praticare la sorveglianza di massa contro gli europei. Istituiscono un ufficio al quale gli europei si possono rivolgere, anche attraverso le autorità Garanti della protezione dei dati personali dei rispettivi paesi, per sapere quali dati su di loro siano in possesso delle autorità americane. E rivedranno l'accordo ogni anno con gli europei, anche per aggiornarlo in relazione all'evoluzione del mondo internettiano.

Le associazioni a tutela della privacy non sembrano del tutto soddisfatte. E Max Schrems, l'attivista che aveva portato con le sue azioni alla decisione della Corte Ue sul Safe Harbour, si dimostra sospettoso sul nuovo accordo. Ma forse va detto, con un pizzico di paradosso, che gli europei rischiano di essere d'ora in poi più protetti in America che in Europa. Non mancano i giuristi che fanno notare che, per esempio, la Cassazione italiana diffonde dati sensibili online, pubblicando le sue sentenze: solo da qualche tempo ha cominciato a oscurare i nomi delle persone coinvolte.


Il Sole 24 ORE

Petrolio, prezzi sotto tiro
Mercati in caduta libera

Fallimenti, duello Tesoro-Giustizia


Economia digitale

Protezione dati, accordo Usa-Ue

Non c'è domenica senza cultura.

CORRIERE DELLA SERA

Data 03-02-2016
Pagina 27
Foglio 1

Il caso

Privacy e datagate intesa Europa-Usa

di **Francesca Basso**

Tutto era cominciato con un giovane studente austriaco che aveva chiesto di bloccare il trasferimento dei propri dati personali nei server statunitensi di Facebook, contestando la sicurezza americana dopo lo scandalo del «datagate», la sorveglianza globale scoperchiata da Snowden. La Corte di Giustizia Ue, interpellata perché è l'unico organo che può dichiarare invalido un atto dell'Unione, in ottobre ha dichiarato illegale il regime «Safe Harbour» (approdo sicuro), l'accordo tra Ue e Usa che per quindici anni ha consentito alle aziende americane di spostare i dati personali degli utenti europei sui server americani. Si è creata così un'incertezza in un ambito dal quale dipendono migliaia di aziende che trasferiscono dati da una sponda all'altra dell'Atlantico, a cominciare da Google e Apple. Da quel momento è partito un negoziato per raggiungere un nuovo accordo, considerato che la privacy è un diritto riconosciuto in modo diverso in Europa e negli Usa. E soprattutto tenuto conto dei requisiti indicati dalla Corte di Giustizia Ue. Ieri è stata raggiunta una nuova intesa: la Commissione Ue ha garantito che «proteggerà i diritti fondamentali degli europei quando i loro dati saranno trasferiti negli Stati Uniti e assicurerà certezza legale al business».
L'impegno degli Stati Uniti è stato rafforzato anche da una lettera del direttore dell'Intelligence nazionale Usa, in cui si impegna a evitare «una sorveglianza di massa indiscriminata» dei cittadini Ue quando le loro informazioni saranno trasferite dall'Europa agli Usa. L'accesso delle autorità pubbliche statunitensi per il rispetto della legge e della sicurezza nazionale sarà soggetto a chiari limiti e meccanismi di salvaguardia e di controllo esterno, e queste eccezioni saranno usate solo «quanto necessario» e saranno «proporzionate». Per controllare il rispetto delle regole ogni anno ci sarà una verifica congiunta che includerà anche il capitolo dell'accesso di sicurezza nazionale. Gli attivisti della privacy restano critici e non escludono il rischio di un nuovo intervento della Corte di Giustizia Ue. Per la commissaria alla Giustizia, Vera Jourova, «è un passo unico che gli Usa hanno compiuto per poter ripristinare la fiducia». Ed eliminare l'incertezza è anche un passo per favorire la crescita.


ECONOMIA
Il «re» mondiale dei gestori: «Basta con il breve termine»
Privacy e datagate intesa Europa-Usa
HITACHI

CORRIERE DELLA SERA

Data 09-02-2016
Pagina 21
Foglio 1

L'esperto

«La società è troppo vulnerabile»

di **Serena Danna**

L'ex direttore della Cia Michael Hayden ha dato della cybersecurity una delle migliori definizioni in circolazione: «Raramente nella storia abbiamo avuto a che fare con una questione così importante e allo stesso tempo così poco definita e compresa». A fare chiarezza nella dimensione opaca dell'insicurezza online prova da anni il politologo americano Peter Warren Singer, co-autore insieme con Allan Friedman di *Cybersecurity and Cyberwar: What Everyone Needs to Know*. «La cybersecurity è un tema che riguarda diversi settori del nostro agire privato e pubblico: dalle informazioni personali al commercio fino alla sicurezza globale — dice al *Corriere* Singer —. Rubare soldi sulla carta di credito è un crimine digitale al pari del furto di informazioni sul nuovo jet militare progettato dal governo italiano». Il politologo, ex direttore del Center for 21st Century Security and Intelligence, ricorda che il 97% delle 500 aziende più ricche del mondo secondo *Fortune* (si deduce che siano anche quelle con i migliori reparti di sicurezza informatica) hanno subito almeno un attacco informatico. «Una diffusione così ampia delle minacce può causare all'economia globale perdite pari a un milione di miliardi tra danni e business in fumo». Una cifra che appare quasi «generosa» se si considera che solo nel 2015 sono andati persi 445 miliardi di dollari per salvaguardare la proprietà intellettuale, per i lavori bruciati e per il tempo speso a rimediare i danni. Se è vero che ogni secondo viene scoperto un nuovo software capace di mandare all'aria segreti, infrastrutture e denaro, è impossibile pensare a una soluzione a breve termine. La parola per Singer è *resilienza*: «Non riusciremo mai a fermare tutti gli attacchi cibernetici, però possiamo renderli meno devastanti e studiare i modi per riprenderci tempestivamente». Per lo studioso, il primo passo è documentarsi sui rischi (a questo propositi consiglia due libri sul tema: *Future Crimes* di Marc Goodman e *@Ware* di Shane Harris). «Dobbiamo intendere la cyber sicurezza come una questione che ci riguarda tutti, come la salute pubblica. Dai genitori ai cittadini, bisogna implementare "il cyber igiene": prendere iniziative per proteggere la propria sicurezza online fermerebbe il 90% degli attacchi», spiega. Gli interventi non possono essere solo individuali: «Aziende e governi devono dedicare alla sicurezza online le stesse risorse e la stessa attenzione riservate ad altri aspetti fondamentali della loro attività».

il Fatto Quotidiano
NON RICEVE ALCUN FINANZIAMENTO PUBBLICO

Data 10-02-2016
Pagina 1
Foglio 1 / 2

NUOVI CRIMINI

Dati e password, ora il ricatto corre su Internet

© DELLA SALA A PAG. 14

Virus Basta aprire un'email e tutto il contenuto del pc viene criptato: "Dammi 500 euro, ti restituisco foto, documenti e pdf"

Web, l'ultima frontiera: riscatto per riavere i dati

» VIRGINIA DELLA SALA

Immaginate di accendere il computer e scoprire che il documento Word con la tesi di laurea o un progetto di lavoro, in una sola notte, sia diventato inaccessibile. Immaginate che la stessa cosa sia accaduta alle copie di sicurezza che avete fatto sulla chiavetta Usb o su un hard disk: significa che il vostro computer è stato infettato da uno dei virus più in voga del momento. E la sensazione di ansia e panico che provate è quella che segna il confine tra la necessità di cybersecurity e un attacco di cyberfobia.

UN LIMITE che non è mai stato così labile come ieri, nel *Safer Internet Day*, la giornata mondiale per la sicurezza online. La declinazione italiana dell'evento si è concentrata sul cyberbullismo e sull'uso consapevole dei social network, con Facebook impegnato a distribuire consigli per i genitori e il Movimento 5 Stelle in procinto di presentare una proposta di legge sul cyberbullismo. Quella internazionale è stata invece impegnata a seminare il panico, con un'analisi delle minacce informatiche a cui andremo incontro nei prossimi mesi.

Si parte dalla recente epidemia dei cryptovirus, un tipo di parassita informatico destinato a diffondersi in maniera esponenziale. Una volta in un computer, ne cripta tutti i documenti rendendo impossibile consultarli. A un utente, ad esempio, è arrivato con un allegato via email. In pochi secondi ha codificato il contenuto del Pc, foto, documenti, pdf, video e audio: "Tutti i file sono stati protetti da una crittografia forte con Rsa - 2048" si legge nel messaggio che compare sullo schermo. Chi ha diffuso il virus ha incluso una richiesta di riscatto. "Ci sono due cose che puoi fare: aspettare un miracolo o pagarci 500 dollari per avere indietro i documenti". Oltre al danno, la beffa: la email con il file infetto proveniva dalla commercialista. Non più di due settimane fa, poi, l'azienda informatica Eset ne ha identificato uno che finge di essere Google Chrome, il noto motore di ricerca: quasi impossibile distinguerlo a meno che non se ne controllino le proprietà.

I VIRUS CAMBIANO quindi *mission*: distruggere il contenuto del Pc non basta più, meglio chiedere soldi o rubare dati. Secondo le analisi dell'Osservatorio Information Security & Privacy del Politecnico di Milano, negli ultimi due anni l'80 per cento delle vulnerabilità sul web sono state formate da *malware* (termine che unisce *malicious* e *software* ed indica quindi programmi maligni che infestano e controllano il Pc); il 57 per cento da *phishing* (una vera e propria 'pesca' di dati come quelli per accedere all'*home banking*), e il 37 per cento da attacchi *ransomware*, sistemi che limitano l'accesso ai dispositivi chiedendo un riscatto in denaro. Fenomeno, questo, aumentato del 165 per cento nel 2015. E così almeno un terzo delle grandi aziende ha subito una perdita o un furto di dati negli ultimi dodici mesi. Un business: CryptoLocker, un *ransomware* apparso alla fine del 2013, ha raccolto almeno 3 milioni di dollari prima di essere fermato.

"A una mia amica è stata rubata l'identità per fabbricare una carta di credito Pos, di quelle che non hanno bisogno del Pin perché basta avvicinarla al lettore per effettuare i pagamenti". Gastone Nencini, country manager di Trend Micro, lo ha raccontato durante l'ultima presentazione a Milano del loro rapporto annuale sulla sicurezza. Se aumenta l'uso di Internet e del mobile, aumentano anche le vulnerabilità. Qualche mese fa, due hacker hanno violato il sistema di un'auto senza pilota, in fase sperimentale: era connessa a un cloud, quindi alla Rete. Se entro il 2019 i dispositivi smart casalinghi connessi a Internet saranno circa 2 miliardi (quanti oggi sono smartphone e tablet), salirà anche il numero delle vittime. Secondo il report, già quest'anno ci saranno altri casi *Ashley Madison*, il sito di incontri online i cui iscritti sono stati rivelati al mondo; altri casi simili a quello di Hacking Team, con l'esposizione di documenti e dati delle istituzioni pubbliche. E ci saranno sempre più richieste di riscatto e tentativi di estorsione. "Non aumenteranno più di tanto gli attac-

chi alle aziende - spiega Nencini - Si concentreranno sui singoli utenti, faranno leva sulla manipolazione psicologica, sulla reputazione delle persone, ricorreranno alla cosiddetta ingegneria sociale e costringeranno a pagare sotto ricatto".

I DISPOSITIVI TECNOLOGICI potrebbero essere utilizzati per compiere atti illegali o addirittura per fornire, a insaputa dei consumatori, potenza di calcolo per fabbricare bitcoin, la criptovaluta - moneta digitale - utilizzata per fare affari sul web, che si auto genera con particolari programmi e tanta energia elettrica.

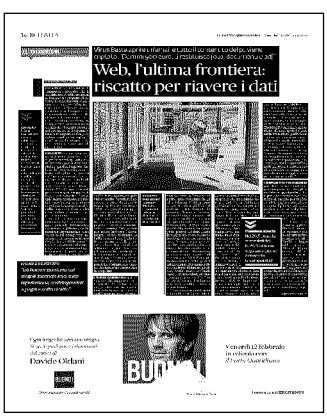
Il futuro non è roseo, quindi: "In Italia manca la cultura della sicurezza informatica, a tutti i livelli - si legge nel rapporto - Meno del 50 per cento delle aziende ha un responsabile di protezione dati e cyber sicurezza". Eppure, secondo le proiezioni, in Europa si apriranno circa 80 mila posizioni lavorative in questo campo. Se ci siano le competenze per coprirle, però, è un altro lungo capitolo.


il Fatto Quotidiano

Sparkle all'uomo di Lotti che rifece la casa a Renzi

TROPPE CAMMELLATE

Pd, la guerra tra i big renziani per 300mila tessere in bianco


Web, l'ultima frontiera: riscatto per riavere i dati

MF

Data 11-02-2016
Pagina 16
Foglio 1

Ancora più difficile gestire la privacy in azienda

DI MARINO LONGONI

Una semplificazione mancata. L'articolo 4 dello statuto dei lavoratori è stato modificato dall'articolo 23 del Jobs act, una norma che si proponeva di adeguare la disciplina dei controlli a distanza sui lavoratori ai nuovi strumenti tecnologici, rendendoli utilizzabili con il minimo di pastoie burocratiche per le imprese. Il risultato è stato un aumento della complessità gestionale e dei dubbi interpretativi.
In particolare, per le apparecchiature da cui può derivare un controllo del lavoratore finalizzato alla tutela del patrimonio aziendale, mentre con le vecchie regole esisteva una giurisprudenza ampiamente consolidata che escludeva la necessità di un accordo sindacale o di un'autorizzazione amministrativa, adesso queste procedure sembrano necessarie. Banalmente, la telecamera per stanare chi prendeva i soldi dalla cassa aziendale è uno strumento di tutela del patrimonio, ma ne può derivare un controllo sul lavoratore: quindi serve l'autorizzazione che prima il 99% delle sentenze considerava inutile.
Sugli strumenti di lavoro la confusione è massima: secondo alcuni quando dall'uso di posta elettronica, smartphone, o del gps sull'auto aziendale può derivare un controllo sul lavoratore, servirebbe la procedura sindacale o l'autorizzazione amministrativa. Pizzetti, ex Garante della privacy, sostiene pubblicamente che se gli strumenti informatici diventano uno strumento di controllo indiretto del lavoratore è necessaria l'autorizzazione o l'accordo. Secondo altri invece il comma 2 dell'articolo 4 basta a escludere questi oneri burocratici per l'azienda, anche perché una lettura diversa finirebbe per svuotare completamente la riforma da ogni effetto di semplificazione. Il ministero del Lavoro finora non ha preso posizione, limitandosi ad affermare che va comunque rispettato il codice della privacy: precisazione poco incisiva perché lo stesso codice ammette che il mancato rispetto delle norme ivi contenute non impedisce comunque al datore di lavoro di utilizzare in giudizio gli elementi raccolti. Alcune grandi società hanno già inoltrato richiesta al ministero di autorizzazione all'installazione di impianti di controllo audiovisivo o geolocalizzazione o app sugli smartphone dei dipendenti (le nuove norme prevedono espressamente la possibilità, per chi ha più sedi sul territorio nazionale, di rivolgere un'unica richiesta a livello nazionale invece di più richieste a livello locale, come era in passato), ma la risposta è stata un gentile diniego e un rinvio alla sede territorialmente competente. Certo, non un grande aiuto.
Il terzo comma dell'articolo 4 dispone invece che le informazioni raccolte con questi strumenti possono essere utilizzate per tutti i fini connessi al rapporto di lavoro, quindi anche per un procedimento disciplinare. A condizione che «sia data al lavoratore adeguata informazione sulle modalità d'uso degli strumenti e di effettuazione dei controlli»
Il datore di lavoro dovrebbe quindi fare una ricognizione degli strumenti di lavoro, degli impianti audiovisivi e di tutti gli strumenti che permettono un controllo a distanza e prevedere un regolamento interno per ciascuno di essi al fine di disciplinare l'utilizzo consentito dall'azienda, elencando anche in modo dettagliato le modalità di controllo che potranno essere poste in essere dall'azienda stessa.
Volendo essere pignoli resterebbe ancora da capire se sugli strumenti di lavoro è necessario attivare anche la procedura di accordo sindacale o autorizzazione amministrativa e se sia necessario anche il consenso del lavoratore per il trattamento dei dati personali. È la chiamano semplificazione! (riproduzione riservata)

Il Sole 24 ORE

Data 14-02-2016
Pagina 18
Foglio 1

Strumenti aziendali. La corporate governance di fronte ai rischi di attacchi informatici

Cybersecurity, la strategia che parte dal vertice

di **Marina Brogi**

Da tre anni il Global Risk Report del World Economic Forum annovera gli attacchi cyber tra i rischi più importanti in termini sia di probabilità di accadimento sia di entità dell'impatto. Le riflessioni durante gli incontri di Davos di quest'anno hanno sottolineato l'importanza di un coordinamento internazionale tra paesi e di un approccio collaborativo tra pubblico e privato per contrastare la criminalità informatica. Per quanto riguarda l'Italia il 4 febbraio è stato presentato il Framework nazionale per la cybersecurity con la partecipazione degli attori principali dell'architettura nazionale governativa per la sicurezza e anche di grandi aziende italiane come Fincantieri, Terna, Luxottica, Intesa Sanpaolo, Snam e Barilla.

Tuttavia, molto si può e si deve fare anche a livello di singola azienda e in particolare, la cyber security è un tema al quale i consigli di amministrazione e i comitati rischi devono dedicare un'attenzione crescente man mano che la tecnologia modifica le combinazioni economico produttive e distributive delle loro società. Per le banche i tempi sono già maturi, la tecnologia ha modificato in modo definitivo sia i processi di back office sia quelli di front office e di rapporto con la clientela e con essi ha intensificato l'incidenza dei rischi informatici e cyber. La banca è accessibile 24 ore su 24 e il cliente assistito dalla sola tecnologia è in grado di svolgere autonomamente moltissime operazioni. Rischio informatico e cyber non riguardano solo i sistemi di supporto alle attività ma si estendono quindi ai canali, ossia all'essenza del rapporto con la clientela, le cui estensioni più recenti in altri paesi includono il roboadvisory ossia l'erogazione di consulenza personalizzata automatizzata. Un ineluttabile e crescente utilizzo della tecnologia nell'interfacciarsi con i clienti di oggi e imprescindibile per farlo con quelli di domani, ossia quegli adolescenti non più teenager ma «screen-ager». Per competere la banca deve migliorare l'accessibilità per il cliente ma è proprio tale maggiore facilità di accesso che si accompagna ad una più ampia possibilità di attacco. Gli strati di pericolo in una app per cellulare sono molteplici, l'hardware, il software (virus), il flusso informativo verso il centro e da ultimo la custodia dei dati nel tempo.

Questo maggior uso della tecnologia pone la banca davanti ad un rischio difficile da misurare, a più bassa probabilità di accadimento rispetto ad altri rischi tipici della banca ma con effetti potenzialmente molto gravi. Un rischio che impone investimenti significativi giustificabili solo se si adotta un'ottica strategica, di orizzonte non breve e che quindi richiede la condivisione del consiglio di amministrazione e l'individuazione e pianificazione degli interventi prioritari.

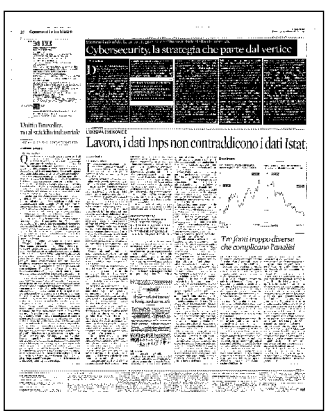
Occorre partire da un'analisi delle proprie strutture, in quanto spesso nel concreto i sistemi informativi si sviluppano rispecchiando le singole esigenze che man mano si manifestano, e non seguendo un disegno unitario. Serve invece ricostruire la catena tecnologica e identificare le eventuali vulnerabilità, quei raccordi fra diversi applicativi che possono essere più facilmente attaccati. Nel definire l'ordine di priorità degli interventi si possono considerare due direttrici guida: a) gli interventi a supporto della catena del valore, ossia l'aumento della consapevolezza del personale con riguardo alle condotte da adottare per aumentare la sicurezza informatica, la mappatura e la messa in sicurezza delle procedure di rapporto con la clientela, la procedura conti correnti, l'home banking e così via; b) gli interventi a supporto della compliance alla normativa, ad esempio l'adeguata verifica, l'antiriciclaggio, e così via.

Da ultimo, la consapevolezza che è molto difficile essere totalmente protetti (come dimostrano gli attacchi anche recenti, l'ultimo ha bloccato l'operatività on line di HSBC un paio di settimane fa) suggerisce la predisposizione ex ante sia di un piano di continuità e disaster recovery, che consenta alla banca di continuare ad operare nonostante l'attacco, sia di un piano di comunicazione e crisis management per informare e rassicurare clienti e mercati.

Estratto della relazione presentata alla Conferenza Internazionale WCD EMEA, Parigi 10-11 febbraio

NESSUNO È TOTALMENTE PROTETTO

La consapevolezza che nessuno può dirsi totalmente protetto (vedi il caso della banca HSBC) deve far scattare piani attenti e preventivi


Cybersecurity, la strategia che parte dal vertice

Lavoro, i dati Inps non contraddicono i dati Istat

la Repubblica

Data 18-02-2016
Pagina 1
Foglio 1

IL CASO

Se Apple sfida l'Fbi nel nome della privacy

"Non possiamo svelare i dati contenuti nell'iPhone del killer"

DAL NOSTRO INVIATO
FEDERICO RAMPINI

SAN FRANCISCO

L'FBI e la magistratura americana minacciano i diritti costituzionali alla privacy del cittadino, in nome della lotta al terrorismo? L'accusa viene da un paladino inatteso delle nostre libertà fondamentali: Tim Cook, chief executive di Apple. Che rifiuta di fornire al giudice federale il codice criptato dell'iPhone usato dai terroristi di San Bernardino. Non importa se quella strage in California il 2 dicembre fece 14 morti, il bilancio più grave di un attacco terroristico sul suolo americano dall'11 settembre 2011. Per il capo di Apple la richiesta di decrittare lo smartphone rappresenta una minaccia troppo grave alla sicurezza di noi utenti. Una volta che Apple avesse fornito all'Fbi il dispositivo per violare il codice crittato, si legge nella lettera che Cook ha divulgato ieri, «potrebbe finire nelle mani sbagliate, che potenzialmente avrebbero accesso a qualsiasi iPhone».

EPPURE la richiesta dell'Fbi è stata passata al vaglio della magistratura, che dopo due mesi di istruttoria l'ha giudicata fondata. L'Fbi sostiene di aver bisogno di aggirare il codice d'accesso e altre funzioni che cancellano automaticamente i dati dell'iPhone, per ricostruire un "vuoto" di 18 minuti negli spostamenti della coppia di terroristi di San Bernardino. Il chief executive di Apple contesta la conclusione del giudice federale. Cook lo accusa di "over-reaching", letteralmente uno sconfinamento. Si tratterebbe solo dell'usare il concetto dell'abuso di potere, ma l'allusione è proprio a quello. Lo scontro tra Apple e la giustizia americana ha già fatto irruzione nella campagna elettorale, com'era prevedibile. Donald Trump è stato il più rapido a impadronirsene. Si è detto indignato del rifiuto di Cook: «Chi si crede di essere?». Ma a suo tempo anche Barack Obama aveva manifestato preoccupazioni per i limiti che i dispositivi di tutela della privacy pongono alle indagini anti-terrorismo. Nel primo discorso alla nazione dopo la strage della California, il presidente aveva dichiarato: «Deve diventare più difficile per i terroristi usare la tecnologia per sfuggire alla giustizia». Da allora diversi summit hanno riunito nella Silicon Valley californiana i massimi responsabili dell'ordine pubblico – il segretario alla Giustizia Loretta Lynch, il direttore dell'Fbi James Comey – insieme con i top manager di Apple, Google, Facebook. Anche i social media sono chiamati in causa: la coppia dei terroristi di San Bernardino aveva una pagina Facebook.

La resistenza "militante" di Cook ha le sue spiegazioni nell'effetto Nsa-gate. Le rivelazioni di Edward Snowden sullo spionaggio digitale della National Security Agency, provocarono dure reazioni in una serie di paesi stranieri, dalla Cina alla Russia, dalla Germania al Brasile. Perfino alcuni governi alleati o amici dell'America, come quello tedesco e brasiliano, allora cominciarono a parlare di costruire dei sistemi alternativi a protezione dei dati dei loro cittadini. È lo scenario di una "nazionalizzazione" di Internet e delle telecomunicazioni digitali, già ampiamente realizzato dai regimi autoritari, ora diventato un po' più verosimile anche altrove. Questa prospettiva crea il massimo allarme nei quartieri generali dei colossi della Silicon Valley, preoccupati di perdere interi pezzi del loro mercato planetario.

Tant'è, fu nel settembre 2014 che Apple rinforzò i codici criptati dei suoi iPhone, elaborando nuovi algoritmi per "mescolare e confondere" i dati del cellulare una volta attivato il codice pin. Gli stessi Padroni della Rete californiani, però, non hanno mai dimostrato altrettanta sollecitudine, nel proteggere la nostra privacy dal saccheggio sistematico di informazioni personali ai fini del marketing e dell'uso commerciale.

Tim Cook accusa il governo Usa di sconfinare e allude all'abuso di potere

la Repubblica

Data 18-02-2016
Pagina 19
Foglio 1

L'INTERVISTA. EVGENY MOROZOV, SOCIOLOGO ESPERTO DI NUOVI MEDIA: "MINARE LA CRITTOGRAFIA NON CI RENDEREBBE PIÙ SICURI"

"Giusto dire no: è a rischio la privacy di tutti"

FRANCESCA DE BENEDETTI

«FA BENE Tim Cook a dire di no al giudice e all'Fbi. Fare breccia nel sistema di sicurezza dell'iPhone dell'assalitore di San Bernardino aprirebbe scenari preoccupanti». Stavolta anche il castigatore di Apple sta con l'azienda di Cupertino. Il sociologo e critico della Rete Evgeny Morozov, 31 anni, bielorusso, ha appena pubblicato in Italia *I signori del silicio* (Codice), ma è anche autore di *Contro Steve Jobs*.

Perché Cook farebbe bene a negare all'Fbi l'accesso ai dati di Syed Farook?

«Per com'è congegnata la sua tecnologia, Apple non può consentire l'accesso limitato ai dati di un solo cellulare. Rispettare l'ordinanza significherebbe creare un sistema che "apra le porte" all'Fbi compromettendo in modo generalizzato la protezione dei dati. E dando così adito a possibili abusi».

Dopo gli ultimi episodi terroristici c'è chi sostiene che serva più sorveglianza, e chi invece difende la crittografia. Ostacolando l'Fbi, Apple non sta mettendo a rischio la sicurezza nazionale?

«Al contrario. Se gli Stati Uniti ottengono l'accesso ai dati, anche altri paesi potrebbero chiedere e ottenere la stessa cosa: un precedente con possibili e pesanti conseguenze geopolitiche. Inoltre, se indebolisci la privacy per favorire l'Fbi, anche qualcun altro potrebbe sfruttare quelle stesse debolezze. Minare la crittografia non rende affatto più sicuri, anzi: una volta create, le *backdoor*, le "porte di servizio", possono essere usate proprio dai terroristi; loro potrebbero finire per sapere su di noi più cose di noi su loro. Senza una risposta convincente a questo argomento, usare episodi di terrore come Parigi o San Bernardino per ampliare la sorveglianza significa secondo me strumentalizzare le tragedie pur di ingigantire a colpi di contratti l'industria della sicurezza».

Proprio lei, il critico della Silicon Valley, sta con Cook?

«Siamo realisti: Apple fa queste scelte per questioni di *brand*, ergendosi a "paladina della privacy". Ma di fatto ci protegge dagli abusi di potere: la storia, e il Datagate in particolare, ci insegna che non possiamo fidarci ciecamente del fatto che l'Fbi non accederà a più dati di quelli strettamente necessari».

In tutto questo, l'Europa che ha appena negoziato uno scudo per la privacy con gli Usa, che ruolo ha?

«È miope. Invece di proporre un business alternativo e sfidare le contraddizioni degli Usa, cede, si adatta fino a smantellare le proprie tutele. E il peggio deve ancora venire. Il direttore dell'Nsa ha annunciato che gli americani sono pronti a "sfruttare al meglio" le possibilità di spionaggio dell'*Internet of things*. Non riusciranno a spiare l'iPhone, ma magari ti controlleranno lo spazzolino smart. Apple è un'eccezione: i poteri economici, oggi, sui nostri dati fondano il loro business».


Il caso
Apple contro Fbi "Non sblocchiamo l'iPhone della strage"
"Giusto dire no: è a rischio la privacy di tutti"

Il Messaggero

Data 18-02-2016
Pagina 15
Foglio 1

L'intervista Alessandro Del Ninno

«La legge Usa non è chiara interverrà la Corte suprema»

ROMA **Avvocato Alessandro Del Ninno, lei si occupa tutti i giorni di tutela della privacy e tecnologie informatiche, ci spiega cosa accade negli Stati Uniti e perché la Apple si rifiuta di collaborare alle indagini?**

«Questo caso torna su un punto particolarmente attuale. Già nell'agosto dello scorso anno una interessante lettera al New York Times del procuratore capo di Manhattan, quello di Parigi, del capo della polizia di Londra e del capo della Corte suprema spagnola, sollevava il caso dicendo che l'utilizzo della crittografia sta ostacolando le indagini in generale e quelle sul terrorismo in particolare. In realtà qui ci troviamo in un caso ancora più specifico. Il giudice qui non chiede solo di esibire i dati, ma di costruire un nuovo software, di modificare il firmware del cellulare in questione in modo che la Fbi possa fare tentativi illimitati di immettere la giusta password e aprire il cellulare, bypassando la cancellazione automatica al decimo tentativo».

Perché Apple si oppone?

«Prima di tutto l'azienda ha comunicato che questo software al momento non esiste, la Apple non ce l'ha. Da settembre 2014, l'azienda ha adottato per tutti i nuovi prodotti una crittografia full disk, per garantire la totale privacy e totale controllo dei propri dati attraverso una tecnologica che neanche il produttore può bypassare e lo stesso farà Android. Apple teme che dopo questo ordine di creare un software per aprire questo cellulare di una generazione leggermente precedente, si chieda di modificare anche i nuovi prodotti, lasciando una cosiddetta backdoor agli investigatori per accedere ai dati».

Non potrebbero semplicemente aprire questo cellulare così importante?

«No, perché neanche loro hanno la password, quando l'utente la sceglie nemmeno il produttore può conoscerla».

Il danno alle indagini però c'è. In tempi di terrorismo internazionale è davvero giusto tutelare la privacy a qualunque costo?

«Dal punto di vista filosofico, è una questione di scelte. E' vero che le indagini possono essere danneggiate, ma è altrettanto vero che in alcuni casi, come dimostra la vicenda Snowden, l'uso massiccio di dati personali ha dato indubbiamente un messaggio sbagliato. Dal punto di vista legale, mancano legislazioni specifiche. Gli stati di New York e della California hanno proposto una legge che imponga alle aziende di costruire software che in alcuni casi consentano agli investigatori di accedere ai dati. A livello federale, c'è invece una nuova norma in senso opposto. Anche in Europa non c'è una normativa precisa su questo punto. Un conto è l'esibizione di qualcosa che un'azienda ha, come nel caso di intercettazioni e tabulati, un conto è obbligare l'azienda a creare un software per accedere ai dati».

Quindi in Italia e in Europa ci sarebbe stato lo stesso problema?

«Probabilmente sì, l'obbligo di "facere" come si dice, al momento non è previsto e secondo me sancirlo significherebbe aprire un fronte pericoloso».

Non si rischia di rendere i terroristi o criminali tecnologicamente più attrezzati degli investigatori?

«Il rischio di danneggiare le indagini esiste, anche se teniamo conto che la crittografia è stata a sua volta introdotta per tutelare gli utenti da alcune forme di delinquenza, come il furto di dati o dentità. Molto probabilmente a questo punto dovrà intervenire la corte suprema per dirimere il caso».

Sara Menafra


Mondo

Apple choc: non violiamo l'iPhone del killer

14

10.000

216

L'esperto Alessandro Del Ninno

«La legge Usa non è chiara interverrà la Corte suprema»

Obama all'attacco di Trump «Non sarà presidente»

Avvenire

Data 18-02-2016
Pagina 19
Foglio 1

L'intervista

«Grave danno per l'azienda aprire quella porta segreta»

Jonathan Zdziarski

NEW YORK

Tecnicamente, quello che l'Fbi chiede alla Apple è fattibile. E la società di Cupertino potrebbe mantenere il possesso del nuovo software richiesto dall'Fbi, senza cederlo al governo. Ma il caso non è così semplice, avverte l'esperto di implicazioni legali della tecnologia Jonathan Zdziarski: le sue conseguenze sono profonde.

Dunque per rispettare l'ordine del tribunale Apple dovrebbe scrivere in tempi brevi un codice personalizzato per entrare nell'iPhone. È così?

Sì, si tratterebbe di una backdoor, una porta sul retro, di fatto un codice nuovo di zecca che comprometterebbe le caratteristiche di sicurezza del telefono. Lo può fare in tempi brevi. Senza quello, gli investigatori federali potrebbero essere in grado di introdursi nel telefono con l'aiuto della Nsa e della Cia, ma ci vorrebbe più tempo.

Apple può limitare il rischio di abusi di potere?

Può configurare il nuovo sistema operativo in modo che funzioni solo sullo specifico iPhone in esame. Potrebbe anche eseguire tutte le operazioni di recupero delle informazioni nei suoi uffici, senza condividere il software con l'Fbi.

Perché il mondo della tecnologia è in tale subbuglio, allora?

Perché questo caso arriva nel bel mezzo di una battaglia tra le aziende della tecnologia informatica e l'applicazione della legge sull'uso della crittografia. Il governo sta cercando di limitare la portata della crittografia, mentre nella Silicon Valley il successo di un'azienda può essere determinato proprio dalla sua capacità di proteggere i dati dei clienti da qualsiasi intrusione. Il problema è venuto alla ribalta dopo che Edward Snowden ha rivelato la misura in cui la tecnologia permetteva al governo di intercettare i dati trasmessi attraverso la rete. Dopo le rivelazioni di Snowden, Facebook, Apple e Twitter hanno dichiarato di non essere più disposte a creare meccanismi che permettano di intercettare dati, appunto, le famose "backdoor". Ora tutti i nuovi iPhone e dispositivi Apple escono dalla fabbrica già crittografati.

Jonathan Zdziarski: «Tecnicamente è possibile. Ma proteggere i clienti dalle intrusioni è il primo obiettivo»

Questo caso creerebbe un precedente?

Non nel senso che altri tribunali non saranno costretti a seguirlo, ma darà al governo più munizioni.

In che modo?

L aFbi, la Nsa e la Cia potrebbero usare questo caso per chiedere al Congresso una legge che consenta l'accesso delle forze dell'ordine a cellulari in caso di necessità. James Comey, il direttore della Fbi, sta già facendo pressione in questo senso. Il Congresso sta analizzando la questione.

Per questo Apple ha detto che l'ordine è pericoloso?

Non solo. Si pone il problema di chi può fare questo tipo di richiesta. Se il governo degli Stati Uniti può costringere Apple a dargli la "chiave" di un telefono, perché non potrebbero farlo i governi cinese o russo? Inoltre, una volta creato questo programma, tutti sapranno che Apple possiede un passepartout per i suoi prodotti e il governo potrebbe esigerlo.

Che cosa succederà adesso?

Questo caso potrebbe spingere le aziende a consentire agli utenti l'accesso alla crittografia infrangibile, così forte che neanche le aziende produttrici la possono rompere.

Elena Molinari

IL MATTINO

Data 18-02-2016
Pagina 9
Foglio 1

«Le multinazionali proprietarie dei dati ormai sono più potenti degli Stati sovrani»

Intervista

Baldoni, direttore del centro Cyber dell'Università La Sapienza «Questo è il primo vero scontro»

Gigi Di Fiore

Professore ordinario di Sistemi distribuiti alla facoltà d'Ingegneria della Sapienza di Roma, Roberto Baldoni è il direttore del Centro di ricerca sulla cyber intelligence e information security.

Professore, su cosa si basa tecnicamente il no della Apple alla richiesta del governo americano?
«Tecnicamente sull'utilizzo del sistema operativo della Apple negli Iphone, a partire dalla versione 8, di dati cifrati legati ad un codice d'accesso individuale. Per entrare nel sistema e conoscere quei dati, è necessario conoscere il codice d'accesso».
L'Fbi non ha un sistema informatico in grado di arrivare al codice e quindi conoscere i dati nell'Iphone?
«No, perché il sistema Apple prevede che, dopo dieci tentativi sbagliati sul codice d'accesso, i dati vengano automaticamente distrutti. Un software che proceda per tentativi matematici viene in questo modo limitato nelle sue prove d'accesso».
All'Apple è stato chiesto quindi di eliminare la limitazione dei dieci tentativi?
«Sì, detta in maniera semplificata è questo. Creare, insomma, una porta oscura riservata che, abbattendo la limitazione di prove sul codice d'accesso, consenta di entrare nel sistema evitando la distruzione dei dati».
La Apple ha il potere di dire no all'accesso a dati utili a un'indagine su un episodio di terrorismo che ha causato 14 morti?
«Rispetto al caso Snowden, legato comunque alle norme del Patriot act seguite all'undici settembre del 2001, ci sono differenze. In quel caso, si giustificò l'invasione della National Security Agency nei sistemi di controllo informatici come forma di prevenzione ad attacchi terroristici. Ora una grande multinazionale, che gestisce dati sensibili globali, può difendere il suo sistema informatico e dire no alla richiesta di violarlo in un Iphone. È evidente che siamo di fronte ad un grande scenario in mutamento».
A cosa si riferisce in particolare?
«Questa vicenda, a mio parere, può essere solo la prima di tanti altri rifiuti delle multinazionali, penso non solo alla Apple, ma anche a Facebook, Amazon con il sistema di archiviazione dati globali nel sistema cloud, Google, Gmail, che gestiscono informazioni a livello mondiale. Questo episodio è il primo serio scontro tra una di queste multinazionali e uno Stato sovrano. Impensabile fino a qualche tempo fa».
Giustificabile in un'indagine delicata su vicende di terrorismo?
«La valutazione etica e l'interesse investigativo è comprensibile, qui probabilmente ci troviamo di fronte all'affermazione di un grande potere globale di multinazionali che hanno ben presente gli interessi di mercato».
Il no difende e afferma l'inviolabilità del sistema Apple?
«Proprio così. È come dire, siamo così sicuri e inviolabili che, senza il nostro intervento, neanche l'Fbi è in grado di entrare nei dati di un singolo Iphone. Naturale che questo dia ancora più forza al software Apple e quindi affermi sul mercato la validità di un prodotto».
È l'inizio di una nuova era?
«Sì, stiamo entrando in una nuova epoca dove l'informazione globale è sempre più un potere in grado di opporsi a Nazioni così forti come gli Stati Uniti. Un potere gestito da grandi multinazionali, che lavorano su scala globale. Si gioca una partita economica molto consistente, che supera altre valutazioni. Questo caso lo dimostra».
Nessun interesse superiore, neanche un'indagine delicata, può scalfire questo grande potere?
«È una bella domanda, che dovrebbe ricevere risposte attraverso regole sui diritti di libertà e privacy. Dovremmo chiederci come mai questa notizia è stata pubblicata in anteprima sul sito web della Apple. C'era interesse a far conoscere il no. Il tema credo sia, ora, il rapporto tra singoli Stati sovrani e potere delle multinazionali. Siamo entrati nell'era del grande scontro tra queste due entità. È un mondo nuovo, molto più complesso e in rapida evoluzione. Credo che da questo episodio nasca un rapporto di forza tra Stati e multinazionali, sbilanciato a favore delle seconde».

> Da questa vicenda nasce un mondo nuovo, la Apple ha fatto prevalere interessi di mercato dando per prima la notizia del suo no all'Fbi

CORRIERE DELLA SERA

Data 18-02-2016
Pagina 1
Foglio 1

PRIVACY E SICUREZZA

PRIMA I CLIENTI POI I CITTADINI LA SCELTA SBAGLIATA DI APPLE

di **Beppe Severgnini**

Apple rifiuta di sbloccare l'iPhone5 del terrorista autore della strage di San Bernardino (14 morti), come richiesto da un giudice federale negli Usa. Non è solo una sottovalutazione: è una provocazione che l'azienda di Cupertino rischia di pagare cara.

Gli Stati Uniti non sono mai stati particolarmente sensibili alle questioni di privacy, come dimostrano i continui litigi tra Google e l'Unione Europea sulla raccolta dei dati e il «diritto all'oblio». La scoperta che la National Security Agency (Nsa), con la silenziosa collaborazione dei colossi del web, spiasse chi voleva, quando voleva, ha destato scandalo all'estero. In America, educate perplessità.

Da dove viene, dunque, quest'improvvisa sensibilità?

La sensazione è che Apple abbia fatto i suoi conti: meglio irritare il proprio governo che spaventare il proprio mercato. Il primo controlla un Paese (gli Usa), il secondo s'estende a tutto il pianeta e genera un fatturato annuale di 234 miliardi di dollari (anno fiscale 2015). L'inviolabilità è un vanto dell'iPhone. Rinunciarvi viene considerata una resa. Commerciale, prima che ideale.

Apple e l'amministrazione Usa duellano sul presente pensando al futuro. Ha scritto Tim Cook: «Il governo ci ha chiesto qualcosa che semplicemente non abbiamo, e consideriamo troppo pericoloso creare. Ci hanno chiesto una versione di iOS (il sistema operativo, *ndr*) che renda possibile aggirare la sicurezza del telefono creando di fatto un accesso secondario all'iPhone».

Risposta: e allora? La protezione dei dati personali è importantissima — come l'Europa tenta da anni di spiegare all'America — ma non è un valore assoluto. Prima viene la vita umana. Banale? Forse. Ma la questione è tutta qui.

Per fermare l'infezione del terrorismo islamista dobbiamo ricorrere a medicine sgradevoli: lo stiamo scoprendo in tanti, dovunque. Intercettazioni, telecamere, controlli ossessivi negli aeroporti. Pensate alla norma (americana) che prevede di dotare il bagaglio di una serratura accessibile alle autorità. Si chiama Tsa, da Transport Security Administration (parte del dipartimento di Homeland Security). Perché accettiamo che il bagaglio venga aperto a campione, da persone anonime, a nostra insaputa? E dovremmo rifiutare che il telefono venga controllato su richiesta precisa e motivata dell'autorità giudiziaria? La risposta non può essere «Perché la Apple ha più potere della Samsonite!».

Edward Snowden aveva ragione a denunciare la sorveglianza indiscriminata, l'interferenza come metodo d'indagine, i controlli a strascico. Tim Cook sbaglia, invece, quando dice: «Nelle mani sbagliate, questo software avrebbe il potenziale di sbloccare qualsiasi iPhone fisicamente in possesso di qualcuno». Le mani dell'autorità giudiziaria non sono sbagliate. Sono le mani autorizzate dal patto sociale, come ha ricordato Massimo Sideri su Corriere.it.

Un'ultima considerazione. La lettera di Apple è intitolata: «A Message to Our Customers», un messaggio ai nostri clienti. Ma i clienti in questione sono anche cittadini. E forse sono prima cittadini da proteggere, poi clienti da accontentare. A meno che Tim Cook pensi di essere il nuovo Thomas Jefferson e voglia cambiare la natura della democrazia in America, e non solo. In questo caso gradiremmo essere informati: basta un messaggio sull'iPhone.


CORRIERE DELLA SERA

Veti, accuse: Renzi gela Berlino

Unioni civili, il voto slitta di 7 giorni


PRIMA I CLIENTI POI I CITTADINI LA SCELTA SBAGLIATA DI APPLE

CORRIERE DELLA SERA

Data 19-02-2016
Pagina 1
Foglio 1

Apple e la giustizia

LA PRIVACY E IL DILEMMA DIGITALE

di **Massimo Gaggi**

Meglio non tracciare linee nette per dividere buoni e cattivi nella *crypto war* tra la Apple (appoggiata dalle altre aziende digitali, a partire da Google) e il governo americano. Intanto perché questa guerra del criptaggio degli iPhone che covava da mesi sotto la cenere viene combattuta attorno a nodi complessi che gli incontri di gennaio del capo dell'Fbi e del ministro della Giustizia Usa con i big della Silicon Valley non sono bastati a sciogliere. E poi perché ogni persona che ha in tasca un iPhone o un cellulare che utilizza Android di Google (il 96% degli smartphone del mondo) vuole che i servizi di sicurezza dispongano di tutti gli strumenti necessari per combattere il terrorismo, ma è anche sensibile alle parole di Tim Cook: creare un sistema per infrangere le difese antihacker di un iPhone significa renderli vulnerabili tutti. Vero, ma è meglio diffidare dei sacerdoti della tecnologia che trasformano un'innovazione (dunque un business) in virtù morale. I campioni della Silicon Valley tendono da sempre a dare alle loro attività un valore etico sociale e di cittadinanza che va molto oltre quello economico, salvo tornare sui propri passi se le convenienze cambiano. È già successo con la privacy liquidata da Zuckerberg come un «valore ormai obsoleto» quando Facebook aveva interesse a infrangerla per motivi commerciali, salvo riscoprirne la centralità quando si è scoperto che i social network erano sorvegliati dai servizi segreti. O con gli occhiali di Google: molto meglio di telefonini giudicati dal cofondatore Sergey Brin strumenti ormai superati.

Quando i *Google Glasses* sembravano ormai prossimi alla commercializzazione, Brin giudicò i cellulari intelligenti strumenti ormai antiquati: oggetti consultati a capo chino, perdendo di vista la realtà circostante e indebolendo le relazioni con gli altri. L'imprenditore parlò addirittura di isolamento sociale da smartphone al quale gli utenti sarebbero sfuggiti grazie agli occhiali digitali che avrebbero consentito loro di cercare dati rimanendo a testa alta. Poi Google ha rinunciato a lanciare i suoi *glasses*. Siamo tornati ai cellulari e dell'«isolamento sociale» da cellulare non si è più parlato. La disputa appena esplosa durerà a lungo e diventerà centrale: gli esperti già considerano criptaggio e sicurezza delle informazioni archiviate nei cellulari la questione più importante fra tutte quelle emerse dall'inizio dell'era digitale: prima ancora che cercare una soluzione è importante, quindi, stabilire il percorso e definire ruoli e rapporti di forza tra gli attori.

Qui è allarmante l'impreparazione e la debolezza della politica americana, paralizzata dalla guerra istituzionale scatenata dai repubblicani contro Obama e incapace di comprendere tempestivamente i cambiamenti di paradigma che derivano dall'introduzione di tecnologie digitali in continua evoluzione. Simbolo di questo ritardo è la stessa ordinanza della Corte federale di Los Angeles che è stata respinta dalla Apple. Per trovare un appiglio giuridico che gli consentisse di obbligare la società di Cupertino a collaborare con l'Fbi, il giudice, Sheri Pym, ha dovuto rispolverare l'All Writs Act del 1789: l'anno in cui iniziò la rivoluzione francese. Oltre a fare ricorso a una legge vecchia di 227 anni, il magistrato la sta usando in modo inedito: fin qui quelle norme erano servite a obbligare una compagnia a consegnare alle autorità informazioni sui clienti già in suo possesso, come nel caso delle società telefoniche che forniscono dati sulle chiamate di utenti sotto indagine. Stavolta, invece, viene chiesto alla Apple di costruire da zero un nuovo software: praticamente un sistema operativo parallelo per realizzare un hackeraggio legale dei sistemi di sicurezza inventati dalla società. Ha ragione Tim Cook quando sottolinea l'anomalia di una situazione nella quale agli stessi ingegneri che hanno creato un sistema di criptaggio che è praticamente una cassaforte a prova di bomba, viene ora chiesto di scassinarla.

Vero, così come è vero che la legge americana più recente sulla collaborazione delle imprese con gli organi di polizia, quella del 1992, non prevede obblighi come quelli dell'ingiunzione del giudice Pym. Ma ciò dipende dall'inedita scelta fatta dalla stessa Apple nel 2014, dopo il caso Snowden, di produrre un sistema di criptaggio che non può essere decrittato nemmeno da chi l'ha creato. Una scelta estrema che andrebbe ridiscussa con le aziende digitali. Tutte allineate a difesa della Apple, ma non necessariamente così compatte. La presa di posizione di Alphabet-Google è arrivata dopo molte ore di silenzio che avevano suscitato una tempesta di interrogativi in rete. E contiene molti verbi al condizionale.


CORRIERE DELLA SERA

Il Papa e Trump, un caso sul voto Usa


UNA CARTA DEI VALORI CON L'ISLAM PER COMBATTERE L'INTEGRALISMO

APRI LA TUA GELATERIA A

4.900€ 7.900€

Il Sole 24 ORE

Data 18-02-2016
Pagina 1
Foglio 1

FBI CONTRO APPLE

Il confine incerto tra libertà e sicurezza

di **Luca de Biase**

L'Fbi chiede che la Apple aggiunga ai suoi iPhone una tecnologia che consenta ai suoi agenti di perquisirli superando i sistemi di protezione della privacy. La Apple rifiuta.

Anche dopo la prima decisione di un giudice federale che ha dato ragione al Bureau. L'amministratore delegato Tim Cook interpreta il suo ruolo di leader culturale nell'epoca della grande trasformazione. L'Fbi gonfia i muscoli legali per difendere la sua posizione tradizionale: non deve esistere nessun sistema di criptaggio digitale più forte della capacità del Bureau di decrittarlo. Ma Cook propone di adottare una visione più coerente con la realtà contemporanea. Entrambe le parti hanno forti motivazioni. Entrambe giocano su argomenti che possono trovare consenso nell'opinione pubblica. Entrambe fanno i loro interessi. Ma dove andrà a finire questa disputa?

L'Fbi vuole usare l'emozione che la strage di San Bernardino ha suscitato nell'opinione pubblica per ottenere consenso intorno a questa ulteriore limitazione della libertà dei cittadini. È una retorica ormai classica: il terrorismo, la criminalità, la follia mettono in pericolo i cittadini e rendono necessarie misure più radicali. Per questo l'Fbi chiede ai cittadini di rinunciare alla libertà in cambio della sicurezza.

Per la Apple questa è una posizione vecchia e ingiusta. La Apple sostiene che i suoi smartphone attuali non possono essere modificati nel modo richiesto dall'Fbi senza mettere in pericolo milioni di utenti innocenti: una porta di accesso aperta per l'Fbi potrebbe essere - e sarebbe - sfruttata anche da criminali, terroristi, potenze straniere, spie industriali e intrusi spinti da ogni genere di interesse commerciale. La Apple sta scegliendo progressivamente di giocare un ruolo di testimone e garante delle policy per la sostenibilità e la privacy. Anche perché Edward Snowden ha rivelato che le agenzie del governo vanno molto oltre i limiti della proporzionalità quando avviano pratiche di sorveglianza. I compratori di iPhone si fidano più della Apple che del governo. Ma il punto è anche più alto: i cittadini che hanno letto di Snowden e che conoscono come funzionano i terminali digitali hanno capito che la loro privacy è anche la loro sicurezza. La Apple intende contribuire alla consapevolezza dei cittadini e non solo dei clienti più avvertiti.

Dal punto di vista legale la vicenda è ancora aperta. Dovesse andare avanti fino alla Corte Suprema, gli avvocati dell'Fbi si troverebbero di fronte a giudici che un paio d'anni fa hanno preso una posizione forte contro le perquisizioni senza mandato della polizia nel telefono personale dei cittadini. Certo, il nuovo caso è diverso. Ma non si può non ricordare che la Corte Suprema aveva votato all'unanimità contro la perquisizione. E che il giudice John Roberts Jr. aveva spiegato la scelta con un argomento che supera il caso specifico, osservando che gli smartphone hanno un ruolo centrale nella vita contemporanea e aggiungendo che «hanno un'importanza tanto pervasiva e capillare nella vita quotidiana che il proverbiale visitatore da Marte sulla Terra potrebbe pensare che i cellulari siano un'importante aspetto dell'anatomia umana». Insomma: il livello della discussione è quello dei diritti umani, non quello delle dispute legali. E spinge a considerare la necessità di aggiornare le questioni dei diritti umani e degli equilibri costituzionali per adattarle a un contesto nel quale una tecnologia ha cambiato tanto radicalmente le condizioni della convivenza civile.

Sulla strage di San Bernardino e sulle innumerevoli stragi compiute da individui americani che sparano all'impazzata sulla gente, il presidente Barack Obama è intervenuto chiedendo l'applicazione di una strategia molto diversa da quella della riduzione della libertà dei cittadini. Tra le altre argomentazioni, il presidente ha suggerito che le armi in vendita negli Stati Uniti siano dotate di chip elettronici che consentano di tracciare chi le sta e dove si trova. Quella sarebbe una forma di controllo ben diversa. Ma sulle limitazioni all'acquisto di armi, gli americani non sentono ragioni. Forse riusciranno invece a riconoscere l'importanza del gesto di Tim Cook. Che su questa storia si gioca l'azienda: in sostanza ha previsto che se dovesse perdere la disputa con l'Fbi i suoi iPhone non sarebbero più sicuri. E a quel punto gli sarebbe difficile tornare indietro.

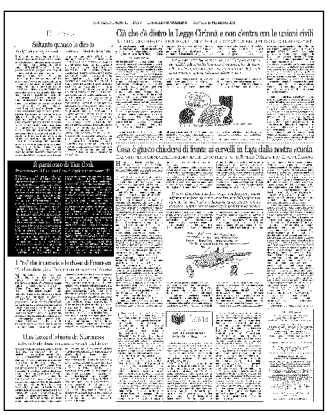
IL FOGLIO

Data 18-02-2016
Pagina 3
Foglio 1

Il paradosso di Tim Cook

Perché in nome della privacy il ceo di Apple si mette contro l'Fbi

L'Fbi americana ha perquisito la casa di Syed Farook e di Tashfeen Malik, i due terroristi autori del massacro di San Bernardino che è costato la vita a 14 persone lo scorso dicembre. Ha interrogato i loro parenti e amici, verificato i loro legami con il jihad internazionale, vagliato le comunicazioni con la Siria. Che debba anche controllare il contenuto dell'iPhone sequestrato di Farook sembra un passo non solo necessario ma anche scontato. Eppure l'Fbi, dopo settimane di tentativi, non riesce ad accedere al dispositivo. Per difendere la privacy dei suoi utenti, Apple (che pure, come tutta la Silicon Valley, fa buon commercio di dati personali) ha dotato i suoi iPhone di una serie di sistemi di protezione invalicabili e si rifiuta di sbloccarli. I federali sono andati da un giudice, che martedì sera ha ordinato ad Apple di fornire gli strumenti per leggere i contenuti dello smartphone incriminato. Cupertino ha ribadito il rifiuto, ha annunciato che combatterà la sentenza e con una lettera "to our customers" del ceo Tim Cook ha trasformato un fatto giudiziario in una questione nazionale. Cook ha scritto che creando un modo per sbloccare l'iPhone di Farook c'è il rischio di generare un sistema per rendere vulnerabili anche tutti gli altri iPhone, una "backdoor". Il governo ci chiede di hackerare i nostri utenti, denuncia Cook drammatico, chiedendo un "dibattito pubblico". Creare una backdoor negli iPhone, effettivamente, potrebbe esporre gli utenti alle minacce di hacker e malintenzionati. Gli esperti ancora discutono se sia questo ciò che il governo chiede, ma intanto la lettera di Cook è bastata per infervorare i toni davanti a una delle più grandi contraddizioni in questi tempi di guerra asimmetrica al terrorismo. Molti governi, tra cui quello francese e quello inglese, hanno approvato o intendono approvare misure che amplificano la capacità di controllo dei dati degli utenti, mentre i giganti della Silicon Valley si schierano a favore di una privacy intransigente. Su questo Cook ha ragione: la questione riguarda decisioni di policy che influenzeranno il dibattito nei prossimi anni. Ma intanto il cellulare di un terrorista conclamato giace inviolato nei cassetti dell'Fbi. Se uno dei contatti dell'iPhone di Farook dovesse fare un attentato terroristico in America, Tim Cook riuscirebbe a mantenere la sua posizione idealista?



la Repubblica

Data 19-02-2016
Pagina 1
Foglio 1

COSA RISCHIAMO SE SI SUPERA IL CONFINE DELLA PRIVACY

JUAN CARLOS DE MARTIN

DOPO mesi di confronti riservati, lo scontro tra il governo americano e i giganti digitali è diventato pubblico, anzi, plateale. Apple ha, infatti, rifiutato di eseguire l'ordine di un giudice federale riguardante l'accesso all'iPhone di uno dei due attentatori di San Bernardino. I dati dell'iPhone, infatti, sono "oscurati" da tecnologie crittografiche che, senza l'aiuto di Apple, l'Fbi non è in grado di penetrare.

La decisione di Apple — spiegata online da una lettera di Tim Cook — ha trovato il consenso degli amministratori delegati di Google e di WhatsApp, oltre che delle associazioni a tutela dei diritti civili come l'Aclu e la Electronic Frontier Foundation.

Cosa sta capitando?

È fuori di dubbio che grazie alla crittografia — una tecnologia ormai utilizzabile da chiunque — è possibile rendere dati (per esempio i file di un computer) o comunicazioni (per esempio uno scambio in chat) inaccessibili a terzi. Questo fatto ha spinto esponenti delle forze dell'ordine a parlare — fin dall'inizio degli anni '90 — del rischio di una «discesa nell'oscurità» di potenziali malfattori. Rischio di cui si è tornati a parlare con insistenza in questi ultimi due anni, dopo che alcune aziende, tra cui proprio Apple, reagendo alle rivelazioni di Edward Snowden, hanno cominciato a inserire nei loro prodotti tecniche crittografiche molto avanzate.

Ha ragione l'Fbi? Apple e altre aziende stanno irresponsabilmente dotando potenziali assassini, mafiosi e terroristi di strumenti inaccessibili alla giustizia?

No, secondo un gruppo di esperti della Harvard University le cose non stanno così. Nel rapporto pubblicato a inizio mese e significativamente intitolato: «Non facciamoci prendere dal panico» («Don't Panic») gli esperti americani (tra cui esponenti di altissimo livello delle agenzie di sicurezza Usa) sottolineano, infatti, che è opportuno considerare la situazione nel suo complesso e non solo lo specifico fatto che alcune comunicazioni possono essere rese impenetrabili dalla crittografia.

> Viviamo già nell'età dell'oro della sorveglianza. Andare oltre sarebbe un colpo mortale alla sicurezza di tutti

E la situazione nel suo complesso — già oggi, ma ancor più in futuro — è più convincentemente descrivibile come un'età dell'oro della sorveglianza più che l'età della «discesa nell'oscurità».

I motivi principali sono quattro.

Il primo è che oggi, a differenza di 25 anni fa, quando è cominciato questo dibattito, ciascuno di noi indossa un dispositivo di tracciamento in tempo reale della propria posizione, noto anche come telefono cellulare. Ne sono derivati enormi benefici per le forze dell'ordine.

Il secondo motivo è che anche se il contenuto di una comunicazione è inaccessibile a causa della crittografia, le informazioni su chi sta chiamando chi, in quale momento e da quale luogo — i cosiddetti metadati — sono invece generalmente accessibili, aiutando molto il contrasto di attività illecite.

Il terzo motivo a sostegno della tesi che viviamo nell'età dell'oro della sorveglianza è che oggi su ciascuno di noi esistono innumerevoli database digitali — dai dati dei social network a quelli finanziari, dalle email agli Sms — che, messi insieme, forniscono un quadro estremamente dettagliato della nostra vita.

Il quarto motivo è che la comunicazione può anche essere crittografata, ma se si riesce ad accedere, con un apposito software di sorveglianza o con una tradizionale intercettazione ambientale (entrambe regolate per legge e approvate da un giudice), allo smartphone o al computer che trasmette o riceve i dati, il gioco è fatto: basta registrare le attività della tastiera (o del microfono, altoparlante, schermo).

Di contro, l'indebolimento della crittografia, come implicito nella richiesta dell'Fbi a Apple o come esplicitamente previsto dalle iniziative di alcuni governi, come quello inglese, sferrerebbe un colpo mortale alla sicurezza di tutti. Come dice, infatti, il noto esperto di sicurezza Bruce Schneier, non è tecnicamente possibile progettare un sistema di sicurezza che funziona solo per persone con una certa cittadinanza o con una determinata moralità: una volta indebolita la crittografia per favorire l'accesso al nostro governo, anche altri governi — magari assai meno democratici del nostro — potranno prima o poi entrare dalla stessa porta, per non parlare di criminali e altri malintenzionati.

Non facciamoci, dunque, prendere dal panico: l'oscurità non sta calando.

Ci saranno, questo sì, angoli più o meno bui. Ma le risorse per gettare fasci potenti di luce non sono mai state così ampie. Così ampie, anzi, da porre il problema — soprattutto con la diffusione della internet delle cose — di come preservare i benefici della rivoluzione digitale senza una pericolosa e generalizzata riduzione della nostra privacy.


la Repubblica

Il Papa: "Neutrale sulle unioni civili e Trump non è un buon cristiano"

Ue, scontro sugli immigrati l'Italia minaccia: meno fondi

"Apple in regola il diritto ai ricordi"


La polemica

"No ai codici all'Fbi" Google e WhatsApp si schierano con Apple

Il Sole 24 ORE

Data 19-02-2016
Pagina 1
Foglio 1

Caso Fbi-Apple: Whatsapp e Google schierati con Tim Cook

Valsania, Melzi d'Eril, Vigevani, Imperiali ▸ pagina 28

Il caso. La «back door» contro il terrorismo richiesta dal Governo Usa sarebbe «un pericoloso precedente»

La Silicon Valley in trincea con Apple contro l'Fbi

Gli ad di WhatsApp e Google si schierano apertamente con l'amico-nemico Tim Cook

di **Marco Valsania**

Google fa fronte comune con Apple nello scontro con l'Fbi e la magistratura americana sulla privacy. L'amministratore delegato del grande rivale del colosso degli iPhone, che da poco l'ha anche superato al primo posto in classifica nella capitalizzazione di Borsa, ha messo da parte ogni astio per sancire un'alleanza in grado di resistere all'ordine di aiutare gli agenti a "sbloccare" gli smartphone e decriptare i loro contenuti in nome della sicurezza nazionale. Un'allenza unisce due aziende che, tra i sistemi operativi Android e iOs, controllano oltre il 90% dei cellulari al mondo. L'amministratore delegato di Google, Sundar Pichai, ha scatenato una serie di tweet in solidarietà con l'amico-nemico Tim Cook. «Obbligare le aziende a permettere l'hacking può compromettere la privacy degli utenti», ha scritto pur riconoscendo le «significative sfide» legate alla protezione del pubblico «da crimine e terrorismo».

Pichai sottolinea che le aziende hi-tech collaborano e intendono continuare a farlo con le autorità federali. «Diamo alle forze di sicurezza accesso a dati sulla base di valide ingiunzioni legali». Ma, rivolto ai consumatori, ha aggiunto che «creiamo i nostri prodotti per mantenere le vostre informazioni al sicuro». Ed è questa protezione che verrebbe messa in dubbio dall'attuale richiesta del governo, fatta propria dal giudice, che impone alle imprese di offrire un sistema per violare tout court la privacy degli utenti, dei loro dati e dei loro apparecchi. Una simile "back door", porta di servizio sempre aperta come l'ha definita Cook, anche a detta del chief executive di Google rappresenterebbe «un preoccupante precedente».

Cook in una lettera aperta aveva spiegato che nei fatti l'Fbi, nel chiedere di aprire l'iPhone 5C dell'attentatore del massacro di San Bernardino, vuole che Apple dia vita a un software ad hoc per gli iPhone, penetrabile dall'esterno, e quindi esposto ad abusi e atti criminali, qualcosa che ritiene «troppo pericoloso per essere creato». L'azione federale è stata definita come un "eccesso" fondato su obsolete norme originarie del Settecento e che darebbero ai giudici potere di autorizzare ampie intrusioni.

Pichai cerca di offrire una via d'uscita al muro contro muro tra aziende e governo e alla dicotomia tra diritti dei consumatori e imperativi di sicurezza nazionale. Una via però stretta e tutta ancora da percorrere. «Mi auguro sia possibile una discussione sincera e approfondita», ha indicato. Il giudice del caso Apple ha dato cinque giorni a Cook per presentare formalmente il ricorso in appello preannunciato nella sua lettera aperta.

Il dibattito promette però di allargarsi, in assenza di nuove norme e legislazioni equilibrate, riprendendo il filo conduttore di altre recenti battaglie, dalla denuncia del generalizzato spionaggio elettronico da parte dei servizi segreti americani da parte del pentito della Nsa Edward Snowden, considerato alternativamente un eroe o un traditore (dal governo), ai recenti nuovi accordi transatlantici sul flusso di dati che rafforzano alcune protezioni per i consumatori sull'onda delle pressioni europee.

Nelle ultime ore le prese di posizione di Silicon Valley, a fianco di Apple, hanno cominciato a susseguirsi al di là di Google: dall'associazione per le libertà civili Electronic Frontier Foundation alla coalizione Reform Government Surveillance che comprende anche Facebook e Microsoft, Mozilla e Twitter. Il fondatore di WhatsApp Jan Koum, oggi parte di Facebook, ha parlato di «libertà in gioco».

È stato tuttavia Snowden, oggi paradossalmente rifugiato in Russia, a offrire il commento forse più controverso e pregnante. «L'Fbi sta creando un mondo dove i cittadini devono contare su Apple per difendere i loro diritti anziché il contrario".

Il Sole 24 ORE

Data 19-02-2016
Pagina 28
Foglio 1

Diritti in conflitto / 1. Il confine tra privacy e sicurezza

In gioco c'è la libertà dei singoli

di **Carlo Melzi d'Eril**
e **Giulio Enea Vigevani**

Ha fatto molto rumore la lettera aperta inviata da Tim Cook, ad di Apple, in seguito alla richiesta del Governo degli Stati Uniti all'azienda di Cupertino di aiutarla a decrittare lo smartphone di un terrorista.

In sintesi: nelle indagini dopo la strage di San Bernardino, gli inquirenti stanno cercando di analizzare i dati presenti nell'iPhone di uno degli attentatori. Tuttavia, per accedere bisogna conoscere la password e dunque il rischio è che dopo alcuni tentativi andati a vuoto il dispositivo – che ha questa funzione – distrugga automaticamente tutte le informazioni che custodisce. Per evitare tale eventualità, che priverebbe la polizia di una possibile fonte importante di spunti investigativi circa i movimenti e i contatti precedenti e successivi alla strage, un giudice ha emesso un'ordinanza con cui chiede a Apple di creare un software che consenta l'accesso alla memoria dell'iPhone in questione. In pratica si tratterebbe di realizzare una "porta" che neutralizzi il meccanismo di cancellazione dei dati e consenta alla Fbi di cercare senza limiti la password.

La lettera di Tim Cook è la risposta negativa a questa richiesta. Allo stato della tecnica non esiste la possibilità di fornire un sistema che "apra" un solo apparecchio; ciò che Apple potrebbe fornire è una sorta di passe-partout per l'accesso a tutti i dispositivi in commercio. E questo non vuole farlo. L'azienda, che sta andando nella direzione opposta, ovvero quella realizzare strumenti dotati di impostazioni sulla privacy che nemmeno il produttore possa eludere, non intende creare un software che permetta di spiare ogni attività effettuata, ogni comunicazione inviata e ricevuta e ogni movimento di ogni singolo possessore di iPhone. Tale passe-partout sarebbe massimamente pericoloso se finisse in possesso di Stati autoritari o di criminali. Ma anche nelle mani della democratica amministrazione americana, conclude Cook, la chiave anti-privacy costituirebbe una minaccia «a quelle stesse libertà che il nostro governo ha il compito e il dovere di proteggere».

Quella che è in atto - e che con buona probabilità finirà sul tavolo della Corte Suprema - è una battaglia giudiziaria all'interno del conflitto forse più drammatico del XXI secolo, quello tra sicurezza e privacy o, meglio, tra sicurezza e libertà dell'individuo. E l'esito finirà con l'incidere non solo sulla relazione tra Stato e individuo, ma altresì sul rapporto di forza tra il sovrano del XX secolo, lo Stato nazionale, e i soggetti che più sembrano insidiare tale predominio, ovvero i giganti delle comunicazioni.

Il dilemma "sicurezza v. privacy" è noto. La tecnologia oggi ha la possibilità di fornire al potere strumenti che consentono un controllo davvero capillare delle "vite degli altri". Dunque, la misura della sorveglianza sugli individui non è più una questione tecnica ma in primo luogo politica e costituzionale.

Da un lato, vi è uno Stato che, invocando le esigenze di lotta alla criminalità e specie al terrorismo, in modo quasi paternalistico chiede a tutti i "cittadini onesti", di sacrificare la segretezza dei propri dati per un bene superiore. Dall'altra, vi è una accresciuta consapevolezza che una progressiva estensione di forme di controllo generalizzate, attraverso il "data mining", finisce con il mortificare la libertà e la dignità dei cittadini. Dunque, lo scontro tra giustizia americana ed Apple può inquadrarsi nel secolare conflitto tra la tendenza degli inquirenti a superare ogni impedimento che ostacoli l'individuazione dei colpevoli dei reati più gravi e la protezione della sfera di libertà dell'individuo.

La novità sono i protagonisti di questo scontro: non lo Stato e i suoi cittadini ma il potere statuale e un altro potere non meno forte, ovvero una grande multinazionale che gestisce dati a livello globale. Ed è probabile che il comportamento di Apple non sia solo ispirato da aneliti libertari: la protezione degli iPhone dalle possibili intrusioni di un governo appare finalizzata principalmente a rafforzare il brand e il rapporto fiduciario con i clienti, a cui Cook non a caso sui rivolge.

In ogni caso, che sia voluto o che sia una eterogenesi dei fini, gli interessi commerciali finiscono con il costituire un baluardo per il cittadino contro la naturale invadenza dello Stato. E confermano dopo due secoli e mezzo, la validità dell'intuizione di Montesquieu che più il potere è diviso, più la libertà dei singoli è salvaguardata.


La Silicon Valley in trincea con Apple contro l'Fbi

In gioco c'è la libertà dei singoli

I limiti e l'ingerenza dello Stato

Il Sole 24 ORE

Data 19-02-2016
Pagina 28
Foglio 1

Diritti in conflitto /2

I limiti e l'ingerenza dello Stato

di **Riccardo e Rosario Imperiali**

L'informazione per divenire notizia deve fare rumore. Il rifiuto di Apple alla richiesta della Fbi di accedere al cellulare dei terroristi che hanno provocato la strage di San Bernardino sa tanto della notizia del padrone che morde il cane. Difficile non esserne coinvolti, difficile non prendere posizione.

Eppure, le libertà non godono del beneficio del palcoscenico alla stessa stregua delle loro violazioni; ed il reiterato cavalcare l'onda dell'emozione di massa, restringendo ambiti e portata dei diritti è tentativo noto. Questi i fatti: per accelerare le indagini relative agli eventi terroristici di San Bernardino l'Fbi, dopo aver ricevuto ampia collaborazione dall'azienda di Cupertino, chiede ad Apple di fabbricare un apposito meccanismo (cosiddetta "backdoor") che consenta al governo ed all'agenzia investigativa di crackare le informazioni contenute nei cellulari dei propri clienti. L'Fbi promette che questa soluzione servirà solo per queste indagini, mentre Apple sostiene che una volta realizzata la backdoor, questa potrà essere utilizzata sempre, come un passpartout capace di aprire qualunque "serratura" digitale. Di fatto verrebbe vanificato il sistema di cifratura utilizzato da Apple per proteggere i dati di traffico e le conversazioni dei propri utenti. Da qui il rifiuto della società che ritiene l'ordine ricevuto sproporzionato e non sorretto da alcuna disposizione di legge. Il governo, di risposta, indica come base normativa della propria richiesta nientemeno che l'All Writs Act del 1789 che autorizza le corti federali ad emettere provvedimenti volti ad agevolare la loro giurisdizione, purchè conformi ai principi di legge.

La coincidenza con la concomitante vicenda del Safe Harbour (cioè l'accordo tra Dipartimento del Commercio Usa e Commissione Ue per il trasferimento di dati personali oltreatlantico) dichiarato invalido dalla Corte di Giustizia Europea è emblematico e fa luce anche su questa vicenda. In quel caso, la Corte ha fondato la propria valutazione di invalidità sulla considerazione che i termini dell'accordo non offrivano sufficienti garanzie nei confronti delle Autorità pubbliche degli Stati Uniti. Ed anzi, il Datagate ha rivelato che «le esigenze afferenti alla sicurezza nazionale, al pubblico interesse e all'osservanza delle leggi statunitensi prevalgono sul regime del Safe Harbour, cosicché le imprese americane sono tenute a disapplicare, senza limiti, le norme di tutela previste da tale regime laddove queste ultime entrino in conflitto con tali esigenze».

Per questi motivi la Corte ha ritenuto che le richieste dell'Autorità pubblica statunitense, in assenza di un equo bilanciamento degli interessi in gioco, fossero da considerarsi eccessive ed in violazione dei limiti al riguardo posti dalla normativa europea. Secondo la giurisprudenza della Corte, infatti, la tutela dei dati personali degli individui è un diritto fondamentale – come riconosciuto dalla Carta di Nizza che ha assunto valore di norma costituzionale – il quale può indietreggiare di fronte ad altri diritti fondamentali come quello alla sicurezza pubblica ma mai sino al suo azzeramento, nel rispetto del principio di proporzionalità. Le limitazioni sono legittime in presenza di precise condizioni: la deroga deve essere necessaria in una società democratica per perseguire uno scopo legittimo, va prevista con una norma di legge formulata in modo preciso e non di contenuto generico. Mentre non sarebbe conforme a questi criteri una norma che, anziché limitare l'ingerenza dello Stato allo stretto necessario, contenesse una generalizzata autorizzazione, senza alcuna differenziazione, limitazione ed eccezione, poiché l'accesso delle autorità pubbliche ai dati e la loro successiva utilizzazione deve necessariamente essere fissato con criteri oggettivi intesi a circoscrivere tale potere. Libertà e diritti vanno presidiati specie nei momenti di elevata emotività sociale ed è emblematico che in questa circostanza si sia trovata in prima linea una multinazionale americana volta a preservare la fiducia dei propri clienti.


La Silicon Valley in trincea con Apple contro l'Fbi
I limiti e l'ingerenza dello Stato

IL FOGLIO

Data 19-02-2016
Pagina 3
Foglio 1

Non solo Apple vs. Fbi. Perché sulla privacy lo scontro è mondiale

LA FAGLIA TRA DIRITTI E SICUREZZA ESISTE DA PRIMA DI TIM COOK. GOOGLE SI SCHIERA, LA VALLEY È DIVISA E PURE LA POLITICA

Roma. La disfida tra Apple e l'Fbi potrebbe finire al Congresso americano e costringere i rappresentanti del popolo a legiferare su una materia da cui finora, nonostante l'urgenza, si sono tenuti volontariamente lontani. Il caso giudiziario potrebbe trascinarsi fino alla Corte suprema, e costringere i giudici a determinare una questione centrale che cambierà profondamente l'equilibrio tra diritti civili e lotta al terrorismo. Ma quella tra Apple e l'Fbi, guerra che si combatte all'incrocio tra privacy e sicurezza, è solo il fenomeno più evidente di una faglia ideologica sempre più frastagliata, di una divisione tra due schieramenti che non riguarda solo l'America e che da tempo è diventata impossibile da ricomporre. I fatti sono noti: la giudice del distretto centrale della California, Sheri Pym, ha firmato un'ordinanza in cui obbliga Apple a sbloccare l'iPhone appartenuto a Syed Rizwan Farook, il terrorista islamico della strage di San Bernardino. Apple protegge i suoi iPhone con sistemi di sicurezza così impenetrabili che nemmeno l'Fbi è riuscita a forzarli, e si è rifiutata di obbedire alle richieste del tribunale dicendo che creare un sistema di sblocco per il singolo iPhone di Farook (una "backdoor") renderebbe vulnerabili tutti gli iPhone del mondo. Con una lettera pubblica che ha fatto molto scalpore, il ceo Tim Cook ha annunciato con toni drammatici che contrasterà l'ordinanza in ogni modo perché ne va della privacy e della sicurezza dei suoi utenti. La statura di Cook come leader d'opinione ha creato un dibattito mondiale.

Nessuno prima di lui aveva espresso con tanta chiarezza la posta in gioco, che è diventata altissima dopo gli attacchi di Parigi dell'anno scorso. E' una questione che ricalca la polemica nata intorno al Patriot Act di George W. Bush, ma rispetto ad allora i sostenitori della privacy hanno molti più argomenti dalla loro parte, e questo rende il confronto più difficile da districare. Da un lato lo scandalo dell'Nsa rivelato da Edward Snowden ha mostrato i presunti abusi del potere governativo nella gestione delle informazioni dei cittadini e instillato il dubbio nei sostenitori della privacy. Dall'altro la scelta tra sicurezza e privacy ha smesso di essere davvero netta, perché in qualunque direzione si vada c'è un pericolo. Dare ai governi e alle forze dell'ordine un accesso privilegiato alle comunicazioni e ai device dei cittadini, attraverso una backdoor o un qualche sistema più ingegnoso, potrebbe rivelarsi un'arma fondamentale nella lotta contro il terrorismo. Avrebbe potuto perfino evitare gli attacchi del 13 novembre a Parigi, come ha detto ieri il direttore dell'Nsa Michael Rogers, inasprendo la polemica. Ma potrebbe al tempo stesso esporci a nuovi e più capillari pericoli, che riguarderebbero questa volta non una singola città ma milioni di persone.

La questione è così inestricabile che gli stessi alfieri dei due schieramenti sono a disagio nelle loro rispettive posizioni. Tim Cook ha scelto il caso più estremo possibile per portare avanti la sua battaglia di princìpi, e rischia di essere additato come protettore involontario dei terroristi. Ma dall'altra parte l'Amministrazione Obama, che si è schierata con l'Fbi e i cui ufficiali da tempo chiedono esplicitamente delle backdoor per bypassare la crittografia dei device (non solo di Apple, ma anche di Google, che nelle ultime versioni suo sistema operativo Android usa delle protezioni simili), teme il contraccolpo davanti al suo elettorato liberal che potrebbe accusarlo di voler ridurre l'estensione dei diritti civili. Dietro di loro, l'opinione pubblica americana, dicono i sondaggi, è divisa perfettamente a metà, e questa divisione non ricalca le linee politiche tradizionali. La frattura tra privacy e sicurezza frammenta gli schieramenti dall'interno. Si prenda il Partito repubblicano. Tutti i candidati alle primarie hanno espresso la loro opinione sul tema e perfino una fazione dentro alla fazione, quella dei candidati più populisti, non è riuscita a mettersi d'accordo. "Chi si credono di essere" quelli di Apple, ha strillato Donald Trump schierandosi deciso a favore dell'Fbi, mentre al contrario Ted Cruz è da sempre un accanito contestatore dei tentativi di controllo della comunicazioni dei cittadini da parte delle forze dell'ordine.

La Silicon Valley e gli interessi economici

Anche la Silicon Valley non è compatta. Il ceo di Google, Sundar Pichai, con alcuni tweet timidi ha espresso il suo sostegno a Cook, ma gli altri giganti del tech, Facebook Microsoft Twitter, stanno zitti a vedere cosa succede. Qui entrano in gioco questioni d'interesse, perché se Apple, che guadagna soprattutto dalla vendita di hardware (ma non solo), può permettersi di posizionarsi commercialmente come "il brand globale della privacy", come ha scritto il columnist del New York Times Farhad Manjoo, le altre compagnie guadagnano soprattutto dalla gestione dei dati degli utenti, e risultano meno credibili come paladine della privacy assoluta propugnata da Cook. Proprio il ceo di Apple, con una mossa velenosa, nei mesi scorsi aveva attaccato duramente il trattamento della privacy di Google, allargando la faglia nel mondo della tecnologia.

Ma anche la stessa Apple entra in contraddizione davanti alla professione di principio del suo ceo. Come ha notato Quartz, Cupertino ingaggia epiche battaglie civili contro il governo americano proprio mentre, in tema di privacy e cessione dei dati, accondiscende alle richieste simili e spesso più esose del repressivo governo cinese – alla stregua di tutte le compagnie tecnologiche americane, che non possono permettersi di perdere il miliardario mercato asiatico. Anche questo è un problema per la Silicon Valley: possiamo pensare di cedere il controllo ai governi democratici dell'occidente, dicono, ma quando sono i regimi a chiederlo? Anche loro dicono di voler combattere il terrorismo, come facciamo a rifiutare? Molti governi autoritari o in aria di autoritarismo, dalla Cina alla Russia, hanno approvato di recente leggi antiterrorismo o leggi sull'"economia digitale" che impongono ampi controlli governativi sui flussi di dati, e di certo se Apple sbloccasse l'iPhone di Farook sarebbero deliziati per il gustoso precedente. Ma anche i governi occidentali, colpiti dalla violenza del terrorismo, dividono le loro opinioni pubbliche con iniziative mirate ad aumentare la sicurezza. L'inserimento dello stato di emergenza in Costituzione da parte del governo socialista francese ha provocato accuse di autoritarismo, mentre gli inglesi sono combattuti davanti alle proposte di regolamentazione di internet del ministro dell'Interno Theresa May, che è arrivata a proporre un controllo capillare delle pagine web visitate da ciascun cittadino.

In tutto il mondo due schieramenti si fronteggiano da tempo l'un contro l'altro armati lungo la faglia ideologica tra sicurezza e privacy. Tim Cook ha solo scoperchiato una pentola il cui contenuto già ribolliva, anche se finora nessun Parlamento e nessun governo ha davvero affrontato direttamente la questione. Se il ceo di Apple ha un merito, è sicuramente quello di aver aperto il dibattito. Tutta ottima pubblicità.

Twitter @eugenio_cau

la Repubblica

Data 20-02-2016
Pagina 15
Foglio 1

L'intervista. Il filosofo Michael Walzer "Non mi fido dei governi, né dei giganti del web. Ma stavolta spiare è sbagliato"

"Non esistono eccezioni se in gioco c'è la privacy di tutti"

ANTONELLO GUERRERA

«Chi ha un'idea precisa su questo tema è un idiota. I governi e i giganti del web sono entità alle quali bisogna stare molto attenti. Ma, se proprio devo schierarmi, stavolta ha ragione Apple». Michael Walzer ha 80 anni, è uno dei massimi filosofi morali contemporanei e, a sorpresa, dà ragione ai giganti della Silicon Valley che non vogliono permettere all'Fbi di entrare nell'iPhone del terrorista di San Bernardino, Syed Farook. Oggi Walzer, eclettico pensatore amato dai liberal e molto ascoltato a destra, teorico della "guerra giusta" che in passato aveva accennato al "paradosso morale" della tortura giustificata in alcuni casi, oggi non cede a nessuna eccezione.

Perché, professor Walzer?

«Perché la posizione di Apple è condivisibile. Hanno fatto il possibile per collaborare con le autorità, vedi la consegna dei file di Farook nel sistema "iCloud". Ma, dovessero cedere adesso, potrebbe aprirsi un precedente pericoloso. Perché non c'è un sistema per decrittare l'iPhone del terrorista preservando la privacy di tutti gli altri. L'eccezione, in questo caso, non è "eccezionale". Se il filosofo Agamben attacca in toto lo "Stato di eccezione" che si verifica negli Stati occidentali in circostanze di "emergenza", mettendo a repentaglio la democrazia, io credo che "l'eccezione" possa essere moralmente accettabile in certi casi. Ma questo non lo è».

Ma entrando nel telefono di Farook si potrebbero magari evitare nuovi attentati e salvare vite. La posizione di Apple è davvero condivisibile?

«Sì. Al momento, non ci sono altre possibilità, come scrive anche il *New York Times*. E poi sulla privacy Apple ha stretto un patto di fedeltà con i propri clienti».

Ma non è un paradosso che Apple e gli altri che si ergono a paladini di privacy e libertà utilizzino dati sensibili potenzialmente infiniti su di noi mentre li negano alle autorità?

«Lo è. Ma c'è una differenza. I giganti del web possono utilizzare i nostri dati a piacimento, come nelle fastidiose pubblicità personalizzate nell'email. Ma non hanno il potere coercitivo dei governi. Apple non può costringermi a comprare prodotti. Un governo, invece, se ha a disposizione dati sensibili, può mettermi in galera. O persino uccidere».

Lei non ha fiducia nelle autorità americane?

«È difficile averne dopo quanto successo negli ultimi anni, vedi lo scandalo Nsa, neanche discusso al Congresso».

E allora che cos'è oggi la privacy per lei che criticò il Patriot Act di Bush che la limitò?

«Non essere spiato con gli amici o in stanza da letto. Ma, devo dirle la verità, non mi dà neanche fastidio se leggono la mia mail. E i sospetti terroristi non devono avere diritto alla privacy. Più in generale, per i cittadini oggi la privacy conta molto meno rispetto al passato. La minaccia terroristica è più importante».

E quindi quali sono oggi i confini tra privacy e sicurezza?

«Purtroppo non so rispondere. Viviamo in tempi troppo fluidi e confusi. Ma il caso Apple-Fbi sarà molto utile a capire questi nuovi confini».

la Repubblica

Data 22-02-2016
Pagina 1
Foglio 1 / 2

"Ecco perché noi di Apple difendiamo i segreti dell'iPhone"

DAL NOSTRO INVIATO
FEDERICO RAMPINI

Il caso

SAN FRANCISCO "CHE ne diresti se ti vendessi una casa, ma tenendomi un mazzo di chiavi da usare a tua insaputa, per entrarci anche quando sarai diventato tu il proprietario? O per darle alla polizia, se me le chiede? Ti sentiresti sicuro? Ti sembrerebbe un trattamento corretto da parte mia, cioè del venditore? E poi, chi ti assicura che quel mazzo di chiavi da me custodito non finisca in mano a un ladro?». La metafora immobiliare la sta usando con me un ingegnere di Apple. Vuole spiegarmi perché, dal suo punto di vista, è assurda la richiesta dell'Fbi e della magistratura americana, di "penetrare" dentro un iPhone. La contesa tra la giustizia americana – cioè in ultima istanza l'Amministrazione Obama – e il colosso digitale della Silicon Valley, dominerà l'attenzione per molto tempo. Spacca l'opinione pubblica, i media e il mondo politico. Tutto ha origine perché l'Fbi vuole il contenuto di un iPhone usato dai due terroristi che fecero strage a San Bernardino, California: 14 morti il 2 dicembre scorso.

Il chief executive di Apple, Tim Cook, ha detto no alle richieste di Fbi e magistratura. Attirandosi un plauso quasi unanime dai media. E la condanna quasi altrettanto unanime dal mondo politico, capace di un'intesa bipartisan pur nel clima arroventato della campagna elettorale. Cook parla solo tramite i suoi legali, ha rifiutato richieste d'interviste da tutti i giornali e tv.

All'interno di Apple vige una segretezza totale, il quartier generale di Cupertino impone regole di comportamento implacabili. L'ingegnere che accetta di parlarmi, un'antica conoscenza per motivi familiari, lo fa a condizione che sia rispettato il suo anonimato. Non rivela segreti industriali; del suo lavoro parla pochissimo, ma si occupa proprio del software per gli iPhone. Mi spiega i ragionamenti che hanno spinto Cook e che lui descrive come ampiamente condivisi da tutti i collaboratori, e anche dalle altre aziende della Silicon Valley, nonché dalla maggioranza degli utenti.

Dunque, proseguiamo con la metafora dell'appartamento. «Ora ci chiedono di poter entrare nel tuo iPhone da una porta di servizio, una porta sul retro. Ma questa porta non esiste, andrebbe costruita ad hoc. Non c'è, o per meglio dire non c'è più un'entrata segreta con cui noi possiamo introdurci nel tuo iPhone a tua insaputa o contro la tua volontà». L'attuale livello di protezione della privacy è relativamente recente. Risale al settembre 2014 cioè al varo del sistema operativo iOS8, nell'era successiva alle rivelazioni di Edward Snowden, cioè lo scandalo detto Nsa-gate. La "gola profonda", il transfuga della National Security Agency, disvelò un livello di cooperazione insospettato fra le grandi aziende tecnologiche degli Usa e i servizi segreti. Ebbe un enorme impatto politico, nel mondo intero. E anche fra gli utenti americani. Per Apple esplose un problema di credibilità, di fiducia presso i clienti. «Da allora – mi spiega l'ingegnere di Cupertino – il codice pin del tuo iPhone è diventato una barriera invalicabile. Io che sono un esperto di iOS8 non posso entrare nel tuo iPhone neanche se lo voglio. E dopo 10 tentativi sbagliati di comporre il pin, automaticamente il tuo iPhone cancella i dati perché si presume che sia finito in mano a un ladro. No, ti assicuro, una porta di servizio non esiste».

Prendo in parola il mio interlocutore e lo seguo nella metafora dell'appartamento. Gli obietto che in casa mia l'Fbi può entrarci eccome, con un mandato del giudice. All'occorrenza sfondando la porta. E nessuno giudica che questa sia una violazione delle libertà costituzionali. In nome della lotta al crimine e al terrorismo, abbiamo accettato regole e procedure che autorizzano una violazione del mio domicilio. Così come la magistratura può autorizzare l'intercettazione delle mie telefonate. La risposta dell'ingegnere di Cupertino: «Quelle regole non si applicano all'iPhone. Ad altri sì. Per esempio l'intercettazione delle telefonate riguarda le telecom, che sono delle utility, dei servizi di pubblico interesse anche quando sono private. Le telecom sono regolate da leggi che non si applicano a noi Apple». Il mio amico ingegnere vota Bernie Sanders, non è un individualista-liberista a oltranza. Ma è convinto che la battaglia del suo capo Cook sia sacrosanta, in difesa di principi fondamentali della democrazia americana.

Il caso Apple-Fbi è già tracimato nella campagna elettorale, con l'appello di Trump a boicottare i prodotti Apple. La politicizzazione è inevitabile. La Silicon Valley, da sempre liberal su temi come l'ambiente e i matrimoni gay, è un serbatoio di voti e di finanziamenti elettorali per i democratici. Tanto che qualcuno si è stupito dello scontro Obama-Cook e ha perfino dubitato che l'Fbi e il Dipartimento di Giustizia non avessero la copertura della Casa Bianca (che invece gliel'ha data). Cook è un personaggio inviso alla destra come pochi: dichiaratamente gay, militante anti-razzista, ha raccontato come la sua coscienza politica maturò nell'infanzia trascorsa tra i razzisti del Ku Klux Klan, in Alabama. I mass media lo stanno appoggiando contro Obama, compreso il progressista *New York Times* che si è schierato dalla parte di Apple. Al Congresso invece democratici e repubblicani potrebbero unirsi e far passare una legge che renda obbligatoria la cooperazione chiesta dal giudice a Cook. Si potrebbe finire davanti alla Corte suprema, essa stessa oggetto di battaglia politica dopo la morte del giudice Scalia. Cook ha già mobilitato due grandi avvocati di sinistra, Ted Olson e Theodore Boutrous, protagonisti della battaglia per i matrimoni gay in California.

LA SCHEDA

LA RICHIESTA

L'Fbi e il giudice chiedono ad Apple un sistema che consenta l'accesso ai dati dell'iPhone 5c di Syed Farook, il killer di San Bernardino

IL NO DI APPLE

Tim Cook, con l'appoggio della Silicon Valley, si oppone: sostiene che creare una "porta sul retro" per quei dati significhi mettere a rischio la privacy di tutti

IL CASO

"PRONTO A TORNARE"

Edward Snowden è pronto a tornare in America "se il governo federale mi garantirà un processo giusto". L'uomo che ha svelato i segreti della Nsa, attualmente in Russia dove ha ottenuto asilo politico temporaneo, lo ha ribadito via Skype durante una conferenza al New Hampshire Liberty Forum

la Repubblica

Data 24-02-2016
Pagina 16
Foglio 1

Fbi, Gates: "Apple dovrà collaborare"

Mr Microsoft: "Ma la privacy si può superare in nome della sicurezza solo seguendo le regole democratiche"

DAL NOSTRO INVIATO
FEDERICO RAMPINI

LAS VEGAS. Bill Gates è su tutte le furie: no, non ha preso posizione a favore dell'Fbi e contro Apple, nella contesa fra tutela della privacy e lotta al terrorismo. Per lui il chief executive Tim Cook ha ragione a pretendere che tutti i livelli della giustizia americana si pronuncino, prima di "violare" il codice criptato dell'iPhone che apparteneva ai due terroristi di San Bernardino. «Una volta seguite le procedure di una democrazia, la privacy può essere oltrepassata in nome della sicurezza nazionale». Il fondatore di Microsoft accusa il *Financial Times* di avere distorto il suo pensiero descrivendolo come un alleato dell'Fbi. Il vero Gates-pensiero, tutti possono verificarlo alla fonte: ascoltando la lunga intervista da lui rilasciata a Charlie Rose e andata in onda lunedì sera sulla rete televisiva pubblica *Pbs*. «Non appoggio una posizione estrema, quella per cui il governo ha sempre ragione e ogni sua richiesta va accolta, come ai tempi in cui Edgar Hoover dirigeva l'Fbi. Ma non mi riconosco neppure nell'idea che il nostro governo sia cieco, quindi impotente di fronte a minacce per la sicurezza nazionale: terrorismo, criminalità, pedofilia».

Gates, che oggi non ha più incarichi operativi alla Microsoft (ma è l'uomo più ricco d'America grazie al suo pacchetto azionario), si dedica a tempo pieno alla fondazione filantropica creata con la moglie Melinda. Resta però un "grande saggio", consultato sui temi dell'economia digitale. Il caso Apple lo vede in una posizione delicata perché per decenni si è alimentata la leggenda sulla rivalità aziendale e anche personale tra lui e lo scomparso Steve Jobs. Ma nell'intervista a Rose, Gates non ha lasciato trasparire animosità. Su un punto solo Gates si dissocia dalla versione di Cook: «Non è vero che la tecnologia per oltrepassare il codice criptato non esiste, non è vero che una volta inserito il pin un iPhone diventa impenetrabile. È come se una banca di fronte alla richiesta di fornire i dati del conto corrente di un cliente, in un'indagine per evasione fiscale, sostenesse di non averli».

Il problema tecnologico è risolvibile. Però Gates, incalzato a più riprese dall'intervistatore di *Pbs*, non si mette contro Cook. In questo si allinea alla posizione di tutti gli altri gruppi dell'economia digitale, da Google a Facebook. Per il fondatore di Microsoft, «siamo in una democrazia e ci sono delle regole, delle procedure da seguire, perché la comunità nazionale si pronunci sull'equilibrio tra privacy e sicurezza». Secondo lui il rifiuto di Apple di obbedire all'Fbi, e al giudice federale, è solo un passo procedurale e garantista, per far sì che la questione venga trattata ai livelli più elevati: in appello e possibilmente fino alla Corte suprema. «È ovvio che quando la Corte suprema si dovesse pronunciare a favore, Apple dovrà collaborare». Gates traccia una distinzione tra governi democratici e regimi autoritari come la Cina. Ricorda che anche fra le democrazie esistono posizioni diverse, citando l'ampia diffusione di videocamere di sorveglianza in Inghilterra. Conclude auspicando che gli Stati Uniti «abbiano un ampia discussione su questo tema, e poi stabiliscano un precedente che sia di esempio anche per altri».


La polemica
Fbi, Gates: "Apple dovrà collaborare"
MOBILE IS VERYTHING
"Violare un iPhone mette a rischio i diritti di tutti"

Il Sole 24 ORE

Data 24-02-2016
Pagina 9
Foglio 1

L'ANALISI

Antonello Soro

La garanzia della privacy un diritto di libertà

EUROPA E STATI UNITI

Il diritto alla protezione dei dati va posto al centro dell'agenda: è la misura della qualità di una democrazia

Per quanto possa non stupire visti i precedenti ai danni di altri Paesi, la notizia delle intercettazioni effettuate dall'Nsa, con modalità ancora da chiarire, nei confronti dell'allora Presidente del Consiglio italiano, se confermata, sarebbe gravissima. Come gravissima è sin da subito apparsa la notizia delle intercettazioni effettuate dalla stessa Nsa, nei confronti di Angela Merkel o Nicolas Sarkozy. In gioco non vi è solo la riservatezza degli interlocutori, quanto piuttosto lo spionaggio politico, realizzato peraltro nei confronti di un Paese alleato.

Ma non meno grave sarebbe, se confermata, la notizia della massiva acquisizione di dati personali realizzata dalla stessa Nsa ai danni di comuni cittadini: 45 milioni di metadati in un solo mese tra il dicembre 2012 e il gennaio 2013. È, questo, un tema che torna oggi all'attenzione, con la stessa drammaticità, a meno di tre anni dalle prime rivelazioni di Snowden. Già all'epoca avevamo sollecitato il Presidente del Consiglio a svolgere una verifica puntuale sulla violazione della privacy dei cittadini italiani e la stessa Ue ha avviato un confronto con gli Usa, per chiarire meglio i contorni della vicenda. L'opposizione del segreto, da parte degli Stati Uniti, su molti degli aspetti centrali del Datagate ha, ovviamente, limitato la possibilità di accertare pienamente la verità, riproponendo quel conflitto tra segreto di Stato e diritti fondamentali oggi, sia pur in altre forme, all'attenzione della Corte europea dei diritti umani per il caso Abu Omar.

E tuttavia, che in nome della lotta al terrorismo si siano compiute, proprio in una democrazia consolidata come gli Usa, gravissime violazioni dei diritti fondamentali, è stato chiarito dalla stessa Commissione parlamentare occupatasi della vicenda. In quella sede si è anche riconosciuto che simili misure di controllo generalizzato sono non solo lesive dei diritti fondamentali ma anche inefficaci, determinando raccolte di dati così massive da risultare poi ingestibili e, quindi, del tutto inutili ai fini di analisi.

Le conclusioni della Commissione Feinstein hanno così agevolato la riforma dell'intelligence voluta da Obama, rafforzando (ma non per chi non sia cittadino americano) le garanzie rispetto all'azione investigativa.

Proprio per impedire ulteriori violazioni dei diritti dei cittadini europei, la Corte di giustizia ha di recente annullato l'accordo Safe Harbour, che legittimava il trasferimento di dati personali verso gli Usa, in ragione delle scarse garanzie che quell'ordinamento offre, sotto il profilo della protezione dati, ai non cittadini. Un primo accordo tra la Commissione e gli Usa ha segnato qualche progresso, ma il tema del diritto alla protezione dati rispetto ad attività d'intelligence così invasive resta. E la domanda di accertamento della verità non può restare inevasa. Per questo è necessario che il Governo anzitutto – e se del caso la magistratura – facciano piena chiarezza su questo punto, accertando non solo la posizione dei nostri Servizi, ma soprattutto quella degli organi d'intelligence stranieri.

E, per prevenire ulteriori violazioni, il diritto alla protezione dati va posto al centro dell'agenda politica, nella consapevolezza che su di esso si misura la qualità della democrazia e da esso dipende la nostra libertà. Sulla protezione dati non può valere il paradigma del nimby (not in my backyard), ovvero l'attenzione a tale diritto solo quando ci riguardi (come Paese, come individui) in prima persona. Come non può, questo diritto fondamentale, essere oggetto di un rispetto solo "presbite", che porti a denunciarne le violazioni perpetrate altrove ma legittimi ogni sua compressione nei nostri confini, per mera convenienza politica. Pensando al paradosso francese della disciplina, in Costituzione, dell'emergenza e delle limitazioni dei diritti fondamentali che può legittimare, c'è da temere che proprio quell'Europa che ha rappresentato un modello verso cui tendere nel rapporto tra libertà e sicurezza, si allontani da se stessa. E da quei principi che ne fondano l'identità: la garanzia della privacy soprattutto, come libertà dal controllo e condizione di una democrazia pluralista e personalista.

Presidente dell'Autorità Garante per la protezione dei dati personali


Wikileaks

Berlusconi spiato dagli Usa, caso diplomatico

Usa preoccupati per i rapporti con la Russia

Abu Omar, Strasburgo condanna l'Italia

l'Unità

Data 24-02-2016
Pagina 4
Foglio 1

Intervista a **Mario Del Pero**

«È l'onda lunga dell'11/9. Ascolti di massa minaccia per tutti»

Lo storico: «Enorme massa di dati soggetta a controlli molto labili»

Francesco Cundari

«È l'onda lunga dell'undici settembre». Mario Del Pero, professore di Storia internazionale a Parigi Sciences Po, ha dedicato diversi libri alla Storia degli Stati Uniti, e uno, con Phillip Deery, proprio al mondo dell'intelligence ai tempi della guerra fredda: *Spiare e tradire* (Feltrinelli). Nel caso politico-diplomatico scoppiato attorno agli ultimi «dispacci» di Wikileaks, Del Pero vede dunque la conferma degli effetti di lungo periodo prodotti dalla reazione agli attentati dell'11 settembre 2001, con il peso preponderante assunto in America dall'intelligence e dalle esigenze di sicurezza nazionale, ma anche il segno di «quanto sia cambiata l'intelligence in questi anni».

In che senso, professore?

«Da due punti di vista. Innanzi tutto, grazie alla tecnologia, che permette di intercettare e archiviare milioni di dati. E in qualche modo, di conseguenza, permette di non discriminare più, perché cattura e immagazzina praticamente tutto. Ma ovviamente si tratta di informazione grezza, non lavorata. Il secondo aspetto significativo è che questo sistema non si fermava davanti a niente. In altre parole, quello che queste rivelazioni confermano è che da anni gli apparati di intelligence americani, e in particolare la Nsa (National security agency, *ndr*), conducevano una campagna di intercettazioni molto invasiva, molto aggressiva, e anche molto poco selettiva: archiviavano milioni di dati sulle comunicazioni in giro per il mondo, accumulando informazioni di ogni genere».

Cosa pensa delle informazioni emerse a quest'ultimo giro?

«Come spesso accade, anche per quanto stavamo dicendo, nel merito si tratta di informazioni che già conoscevamo, che avevamo già letto su tutti i giornali. E cioè che l'Italia, dopo l'esplosione della crisi economica mondiale nel 2008, è stata per una certa fase un'osservata speciale, in particolare per gli Stati Uniti, preoccupati della tenuta dell'Europa e quindi del nostro paese, visto come l'anello debole, anche per l'azione, o l'inazione, del governo Berlusconi. Insomma, che in particolare nel 2011 ci fossero queste preoccupazioni negli Stati Uniti e in Europa non lo scopriamo oggi, così come non scopriamo oggi che Sarkozy tendesse a scaricare tutto sull'Italia per coprire i problemi della Francia».

Quello che scopriamo, se non oggi, da quando è scoppiato il caso Wikileaks, è che persino i nostri vertici politico-istituzionali erano spiati. O forse la vera novità di questa fase è proprio il fatto che lo scopriamo, che il fatto diventa di dominio pubblico, il che pone evidentemente anche un inedito problema politico-diplomatico?

«Diciamo che prima era un processo più controllato e più controllabile, in cui difficilmente un primo ministro si sarebbe trovato nella condizione di Matteo Renzi oggi, o Angela Merkel a suo tempo».

Il paradosso è che quella stessa tecnologia che permette le intercettazioni di massa è anche alla base della loro rivelazione.

«E c'è anche il paradosso di apparati di intelligence sempre più invasivi, che fanno ampio uso di una "tecnologia facile", apparati che operano con sempre maggiore discrezionalità, in sistemi di comunicazione sempre più porosi. Se poi a tutto questo aggiungiamo la tendenza ad affidare una parte crescente delle attività di intelligence in outsourcing, si capisce che, crescendo il numero delle persone coinvolte e dei contractor esterni che hanno accesso a questa enorme massa di dati, mantenerli segreti si fa sempre più difficile. Edgar Snowden, per fare solo un esempio, non era un funzionario pubblico. Ma uno Stato che delega o subappalta questo lavoro a privati, evidentemente, è uno Stato che si fa più vulnerabile...».

Sta dicendo che in questa vicenda si può leggere anche un segnale di debolezza degli Stati Uniti?

«Beh, fossero così forti, tutelerebbero meglio i propri segreti».

Resta il fatto che quanto è emerso appare piuttosto grave...

«Io credo che il problema principale sia quello della privacy, chiamiamolo così, in mancanza di un termine migliore. E cioè che ci sono agenzie di intelligence in grado di catturare e archiviare per un tempo lunghissimo, praticamente infinito, miliardi di intercettazioni che di fatto coinvolgono tutti noi. Tra parentesi: anche in virtù della parziale privatizzazione di questo processo, la gestione di questa enorme massa di dati è soggetta a forme di controllo e regolazione sempre più labili. Questa è la cosa che più preoccupa, molto più del cosiddetto "golpe" contro il governo Berlusconi. Il problema non sono i singoli episodi, ma il sistema di intercettazioni di massa che rivelano, e che rappresentano un pericolo per la democrazia».


Primo piano

Berlusconi spiato
Convocato
l'ambasciatore Usa

«È l'onda lunga dell'11/9. Ascolti di massa minaccia per tutti»

la Repubblica

Data 25-02-2016
Pagina 2
Foglio 1

L'INTERVISTA/ANTONELLO SORO, GARANTE PER LA PRIVACY

"Inevitabile un intervento il problema è la raccolta dati nessuno sa chi e come li usa"

STEFANIA MAURIZI

ROMA. «Credo che questa vicenda dovrebbe servire per rimettere al centro di un'agenda intelligente il tema della protezione dei dati». All'indomani del terremoto innescato dalle intercettazioni dell'Nsa su Silvio Berlusconi e i suoi più stretti collaboratori, il presidente dell'Autorità Garante per la Privacy, Antonello Soro, sottolinea come il problema più grave sia la raccolta massiva di informazioni operata dalla Nsa. E biasima un atteggiamento schizofrenico verso questo tema. «Solo quando riguarda la nostra persona, o comunque noi come individui o come stato, il valore di questo diritto viene percepito come fondamentale e magari chiediamo al Garante di esercitare un'energica tutela. Poi, quando è in gioco la vita privata degli altri, la privacy viene declinata come un inutile privilegio individuale, che deve essere recessivo rispetto a ben altre necessità della comunità».

Si aspettava che la Nsa arrivasse ad intercettare figure apicali del governo italiano?

«Pur non essendo chiarissime tutte le modalità, devo dire che la notizia non mi sorprenderebbe, perché appariva inverosimile che l'Agenzia avesse intercettato i vertici del governo di Germania e Francia e non avesse curiosato nelle conversazioni di palazzo Chigi. A suo tempo, avevo chiesto all'allora presidente del Consiglio di fare tutti gli accertamenti necessari. Noi avevamo valutato due aspetti: la violazione delle comunicazioni di un governo alleato, che è una cosa molto grave, pone problemi politici e diplomatici, rappresentando un'interferenza illecita. Ma l'altro aspetto, quello per cui ci siamo preoccupati allora come oggi, è la raccolta massiva che avrebbe interessato anche il nostro paese con l'immagazzinamento in un solo mese - a cavallo delle vacanze di Natale del 2012 - dei metadati di 45milioni di telefonate. Sappiamo che queste raccolte massive non sono solo dannose, ma sono anche inutili: nella lotta al terrorismo, ciò che è mancato non sono le informazioni, ma una raccolta efficace, che non è quella indiscriminata. Il Datagate non ha trovato risposte adeguate: a suo tempo, gli Stati Uniti hanno opposto il segreto su molti aspetti importanti. E devo dire che, come spesso accade, è subentrato uno stato di globale rassegnazione alla condizione della sorveglianza».

Secondo i file di Snowden, l'Italia ha un accordo segreto con il gemello inglese della Nsa, il Gchq, per la condivisione di parte delle informazioni ottenute con alcuni dei suoi programmi di sorveglianza di massa. I nostri servizi d'intelligence, però, hanno sempre smentito. Voi avete un protocollo di intesa con loro proprio in tema di protezione dei dati, lei esclude complicità?

«La mia esperienza di collaborazione con l'attuale dirigenza dei servizi è stata fruttuosa: non ho ragione di avere dubbi sulla loro serietà, sulla responsabilità e anche, come dire, sulla fedeltà ai valori della nostra democrazia, dopodiché non ho gli elementi per una risposta conclusiva, perché il quesito che lei mi pone riguarda un'esperienza che è al di fuori della mia competenza».

Il Garante ha strumenti efficaci per lottare contro questi programmi?

«Il Garante italiano, come tutte le autorità europee, ha molti strumenti, che discendono dalle norme, ma la struttura è assolutamente sottodimensionata rispetto alla sfida che abbiamo davanti».

VICENDA UTILE

Questa vicenda dovrebbe servire per rimettere al centro dell'agenda il tema della protezione dei dati


WikiLeaks
Boschi: "Inaccettabile spiare Berlusconi" I pm aprono l'inchiesta
"Inevitabile un intervento il problema è la raccolta dati nessuno sa chi e come li usa"

LA STAMPA

Data 26-02-2016
Pagina 1
Foglio 1

DIPLOMAZIA DEI DIRITTI

Sorpresa, gli Usa difensori della privacy

MASSIMO RUSSO

Il nome è in apparenza neutro, «legge sul ricorso giurisdizionale». Ma la norma approvata dal Congresso degli Stati Uniti ci riguarda da vicino e ha in sé l'affermazione di una leadership economica e culturale planetaria. Non attraverso la forza, ma con l'allargamento dei diritti. Il terreno su cui si dispiega questo disegno è costituito dai dati personali. Il riconoscimento dell'*habeas data* - il diritto del singolo a disporre delle informazioni che lo riguardano - significa per il 21° secolo quel che l'*habeas corpus* fu nel Medio Evo.

Allora il diritto a non essere privati della libertà senza il pronunciamento di un giudice naturale significò la fine dell'arbitrio. Oggi la legge firmata dal presidente Barack Obama riconosce ai cittadini delle nazioni alleate la medesima tutela della privacy prima accordata ai soli americani. D'ora in poi noi europei potremo far causa alle agenzie governative Usa qualora esse ci abbiano spiato o abbiano utilizzato i nostri dati in modo improprio. Il provvedimento nasce dalla necessità di ristabilire la fiducia sulle due sponde dell'Atlantico dopo il caso di Edward Snowden, che con le sue rivelazioni tre anni fa rese ufficiale ciò che da tempo era voce corrente: la pratica delle intercettazioni, del monitoraggio e della raccolta di dati personali a strascico provenienti da conversazioni e posta elettronica da parte della *National security agency* (Nsa) e di altri organismi federali. Uno scandalo di cui si è tornati a parlare proprio in questi giorni, con la pubblicazione da parte di Wikileaks dei rapporti che provano come anche Silvio Berlusconi e il suo staff di governo fossero intercettati.

L'apertura, vista dalla prospettiva americana, è un deciso cambio di tendenza rispetto al passato e comporta alcuni rischi: ora uno straniero avrà una base giuridica per portare in giudizio l'amministrazione. Inoltre diventeranno più difficili gli accertamenti nei confronti degli europei sospettati di terrorismo, verso i quali prima esisteva una sorta di libera licenza di intercettazione. Tuttavia la legge risponde a un chiaro disegno strategico: in un'economia globalizzata, garantire diritti anche a non cittadini rende più appetibile per le grandi aziende multinazionali e per gli *over the top*, le grandi piattaforme digitali, insediarsi negli Stati Uniti. Il provvedimento inoltre toglie forza e ragioni a quanti in Europa si erano battuti affinché gli Usa non fossero più considerati *safe harbor*, un porto sicuro per la conservazione e il trattamento delle informazioni di milioni di clienti delle multinazionali.

Il messaggio è semplice: se vuoi cogliere le straordinarie opportunità offerte dalla digitalizzazione dell'economia, il tuo orizzonte non sono più i confini nazionali. Dunque il soggetto destinatario dei diritti non sono più i tuoi cittadini, ma i potenziali consumatori globali. Che devi conquistare con la moneta della fiducia.

Ribaltando il punto di vista, le prerogative di cui godiamo noi singoli non sono più determinate solo dal passaporto che abbiamo in tasca, ma anche dalle nostre scelte di consumo. Un tema tanto più rilevante in vista dell'approvazione del nuovo Accordo transatlantico sul commercio e gli investimenti (Ttip), che tra Europa e Usa formerà il più grande spazio di commercio e scambio al mondo.

A questa sfida il Vecchio Continente si presenta in ordine sparso. Il commissario Ue per la Giustizia Vera Jourová ha plaudito alla legge, definendola «un progresso storico degli sforzi per ripristinare la fiducia nei flussi di dati transatlantici». Ma l'Unione arriva all'appuntamento ancora frammentata in 28 ordinamenti, con altrettante autorità di garanzia, e addirittura con l'ipotesi di ricostituire i confini interni. Un ritardo reso ancor più grave dal fatto che protagonisti della partita non sono più solo gli Stati ma anche le imprese. Il conflitto tra Apple e Fbi di questi giorni, con la società che resiste alla richiesta di rendere accessibili le informazioni contenute nei nostri telefoni, ci parla proprio di questo. Su dati personali, diritti e fiducia, si gioca uno scontro chiave. Lo vincerà chi riuscirà a convincerci di garantirli meglio.

@massimo_russo


LA STAMPA

Le unioni civili passano al Senato con il sì di Verdini

Migranti, Atene sfida il blocco nei Balcani


INCAPACI DI AFFRONTARE LE EMERGENZE

SORPRESA, GLI USA DIFENSORI DELLA PRIVACY

LE CONTESTAZIONI SONO FIGLIE DELL'IGNORANZA

Il Sole 24 ORE

Data 28-02-2016
Pagina 1
Foglio 1

IL CASO APPLE

Un «nuovo» Stato per tutelare la privacy

Un «nuovo» Stato per tutelare la privacy

di **Guido Rossi**

Mentre alcune previsioni di autorevoli economisti lasciano poche speranze per un radicale cambiamento del futuro, entrati come saremmo nell'era della stagnazione secolare, i poteri politici nel mondo si presentano con ancor maggiori inquietanti incertezze.

Poco più di una settimana fa negli Stati Uniti si è scatenata una furiosa battaglia tra la società Apple e l'Fbi sul diritto a controllare i codici criptati degli smartphone. La guerra al terrorismo ha giustificato la richiesta dell'Fbi a conoscere le modalità per decriptare l'iphone di uno degli assassini della strage avvenuta nel mese di dicembre a San Bernardino in California. Il momento più delicato si è verificato il 16 febbraio quando un magistrato federale ha ordinato ad Apple di aiutare l'Fbi a decriptare il telefono in questione.

Continua ▸ pagina 20

IL CASO APPLE

di **Guido Rossi**

▸ Continua da pagina 1

Apple ha nuovamente rifiutato, con un duro messaggio di Tim Cook diretto agli utenti di Apple, dichiarando esplicitamente che il problema è molto più ampio di quanto rappresenti legalmente questo caso, sicché è il momento di aprire una pubblica discussione sul rapporto tra la sicurezza, che deve essere garantita dallo Stato e il diritto alla privacy.

Basti pensare che oggi gli smartphone contengono una quantità di dati personali, dalla propria corrispondenza, alle fotografie, al luogo dove ci si trova, ai pagamenti, ai discorsi segreti e riservati, di cui non v'è traccia altrove.

Tutto il sistema di protezione della privacy da un lato crollerebbe immediatamente qualora Apple fosse obbligata a rompere i propri sistemi di sicurezza, per entrare all'interno di un telefono che la stessa Apple aveva promesso inviolabile ai suoi clienti. E questo costituirebbe tra l'altro un precedente pericoloso al quale poi sarebbe difficile per Apple sottrarsi sia negli Stati Uniti sia negli altri Paesi dove opera, come ad esempio in Cina.

Ed è ovvio che il problema, a seconda di come verrà risolto, riguarda il futuro di una società, come ha sottolineato il prof. Neil Richards nel libro *Intellectual Privacy*, sottoposta ai pericoli di una tecnologia e di un diritto che insieme cospirano ad eliminare la possibilità di pensare senza timore di essere sorvegliati. Stuoli di avvocati, da una parte e dall'altra, si stanno preparando all'udienza in Corte, che si terrà il 22 marzo, ma che sarà ben difficilmente quella definitiva, considerato che entrambe le parti hanno dichiarato che ricorreranno alla Corte Suprema.

Quanto poi all'alternativa "sicurezza garantita dallo Stato e tutela privata della privacy", il problema è aperto fin dal 2013, quando le rivelazioni di Edward Snowden resero pubblica la continua violazione della privacy. Proprio le rivelazioni di Snowden hanno dimostrato che il governo americano non può essere creduto di non abusare dei propri poteri di sorveglianza. È altresì vero che Apple ha fatto della privacy e della sicurezza della protezione dei dati personali uno strumento di grande rilievo e importanza per la vendita dei suoi prodotti.

Come ha indicato Michael Walzer, uno dei maggiori filosofi americani, le società come Apple non hanno il potere coercitivo dei governi, né possono costringere a comprare i loro prodotti. I governi, le forze dell'ordine e la magistratura viceversa possono mettere in galera e persino uccidere. D'altra parte Lawrence Lessig aveva già da tempo messo in guardia dai rischi di una società dell'informazione, meno libera e più feudale.

La soluzione di questi problemi, di una complessità tecnologica oltreché legale notevoli, condurrà probabilmente, in questa nostra era di incertezza e di paura, al ripensamento dei poteri pubblici e degli Stati, con la conseguente soluzione del dilemma "sicurezza contro privacy" per una nuova società che sia in grado di imbrigliare quel potere industrial militare, come lo aveva definito con grande lucidità il presidente Eisenhower, trasformatosi poi in quello attuale ben più brutale "finanza-tecnologia".

Il Messaggero

Data 29-02-2016
Pagina 1
Foglio 1

Sicurezza e privacy

Apple-Fbi dati da svelare proibita solo la diffusione

Carlo Nordio

Il conflitto che oppone Apple al Fbi può, grossolanamente riassumersi così. Gli investigatori federali hanno chiesto all'azienda di creare un software per decrittare il cellulare posseduto dall'autore della strage di San Bernardino. Apple ha rifiutato, sostenendo che costituirebbe una violazione della segretezza dei dati, e un pericoloso precedente che potrebbe condurre a uno "Stato di polizia".

Un giudice ha, provvisoriamente, dato ragione al Fbi. Bill Gates ha suggerito all'azienda di collaborare. Ma varie associazioni di giuristi, informatici eccetera, hanno protestato. Certamente il conflitto finirà alla Corte Suprema.

Il caso non ci interessa direttamente. In Italia sono così tante le intercettazioni in atto, che non c'è bisogno di chiedere la ricostruzione dei dati: ce li prendiamo direttamente dagli interessati mentre parlano o scrivono. Ma negli Stati Uniti dove, come in tutto il resto del mondo civile, le intercettazioni sono rare ed eccezionali, il problema si è posto nella sua reale portata, e le sue implicazioni sono di interesse universale. Proviamo a spiegarle in poche righe.

Primo. L'esperienza insegna che quello che la tecnologia consente di fare, prima o dopo si fa. Questo vale per la bomba atomica, per la manipolazione genetica e, nel caso concreto, per la captazione di dati sensibili. Oggi - è bene che lo sappiamo - qualsiasi conversazione (orale, telefonica oppure telematica) può essere intercettata.

Certo, i vari servizi di spionaggio non spenderanno soldi ed energie per registrare dal satellite un volgare ladruncolo. Ma se volessero, potrebbero. Anche se il sospettato parlasse in un bunker ascoltando, a tutto volume, la quinta di Beethoven. Pertanto, quando comunichiamo, lo facciamo a nostro rischio. Insomma, siamo avvertiti.

Secondo. Tutte le scelte della vita sono frutto di un bilanciamento di valori, o meglio di interessi. Possono essere etici, religiosi, economici, aziendali, sentimentali, ma sono sempre interessi. Nel caso di cui parliamo, l'interesse alla riservatezza dei dati è opposto a quello della ricostruzione di una strage e dell'individuazione dei complici del colpevole, peraltro deceduto. Quale dei due è prevalente? Personalmente credo che negli Usa, come in Italia, il diritto alla riservatezza debba cedere di fronte a due valori, e a due soltanto: la sicurezza nazionale e l'incolumità pubblica o privata. Ma quale che sia il verdetto finale della giustizia americana, si tratta, in definitiva, di una scelta politica. Per l'Italia sarebbe opportuno che il legislatore definisse chiaramente gli interessi ai quali possa esser sacrificata la segretezza delle comunicazioni, bene primario protetto dall'art 15 della Costituzione.

Terzo. Il problema della "detenzione" dei dati sensibili, è in realtà un falso problema. Se Apple non vuole concederne l'accesso al Fbi, sbloccando il cellulare, i confini della disputa sono solo spostati. Perché con il pretesto di evitarne la consegna, Apple ne mantiene il monopolio esclusivo. Anche se le conversazioni non saranno ricostruite dall'Agenzia federale, potranno benissimo esserlo dall'azienda privata. Sarà dunque una segretezza affievolita e precaria, perché nessuno può garantire che un giorno un dipendente infedele non decritti i messaggi e, come è accaduto con WikiLeaks, li passi alla stampa.

Questo ci conduce all'ultima considerazione, valida anche per noi. Che il problema vero non è tanto la "detenzione" dei dati sensibili - intercettazioni o altro - ma la possibilità di una loro diffusione. Non vi è nulla di male che lo Stato ascolti, nell'interesse della sicurezza e dell'incolumità pubblica, tutte le conversazioni che ritiene utili. Anzi, è bene che a tal fine disponga di mezzi sempre più aggiornati ed efficienti. Ciò che dev'essere impedito è che ne faccia un uso improprio e, peggio ancora, che ne consenta la pubblicazione. Il nostro ordinamento prevede già questo saggio bilanciamento di interessi. Si chiamano "intercettazioni preventive", costituiscono un ottimo strumento di controllo, costano relativamente poco e soprattutto, essendo nella cassaforte del Pubblico Ministero, sotto la sua personale responsabilità, non finiscono mai sulla stampa. Come invece è accaduto occasionalmente con WikiLeaks, e come da noi, per le intercettazioni ordinarie, accade quasi ogni giorno.


Il Messaggero

Adozioni gay, il caso che divide

Maxistipendi nelle Regioni Così gli enti aggirano i tetti

LA STAMPA

Data 01-03-2016
Pagina 29
Foglio 1

Le nuove regole varate da Bruxelles

Al via lo scudo per la privacy Proteggerà i dati dei cittadini Ue

Saranno ammessi i ricorsi e l'accesso ai contenziosi

EMANUELE BONINI
BRUXELLES

Oggi cominciamo a tradurre in realtà lo scudo per la privacy». E' Andrus Ansip, commissario Ue per il Mercato unico digitale, a tenere a battesimo il varo delle nuove regole per il trattamento dei dati personali tra Ue e Stati Uniti. Lo hanno chiamato «Scudo» perché intende proteggere le informazioni individuali dei cittadini europei da «accessi generalizzati». In tempi di rivelazioni su spionaggi e controlli da parte dei servizi di sicurezza statunitensi, le regole appena disegnate intendono segnare una chiara inversione di rotta, in quanto «escludono qualsiasi atto di sorveglianza di massa o indiscriminata».

Il testo che genera lo «Scudo» è stato presentato ieri a Bruxelles. Per la prima volta gli Stati Uniti hanno dato all'Ue garanzia scritta, firmata dall'Ufficio del direttore dell'intelligence nazionale, che «tutti i diritti di accesso delle autorità pubbliche ai fini della sicurezza nazionale saranno soggetti a precisi limiti, garanzie e meccanismi di controllo». Viene così rispettato l'impegno preso il 2 febbraio scorso, quanto Bruxelles e Washington avevano trovato l'intesa per le nuove regole, dopo che la Corte di Giustizia Ue aveva invalidato le vecchie, raccolte nel defunto «Safe Harbour». Il patto prevede anche obblighi di tutela stringenti per tutte le società Usa che maneggiano i dati personali dei cittadini europei (Amazon e Ebay, solo per citarne alcune) e più potere alle autorità della privacy nel vecchio continente, a cui i cittadini Ue potranno rivolgersi in caso di controversie. Saranno poi le Authority a fare pressione sulla Commissione federale per il commercio perché i contenziosi vengano eliminati. Gli Usa accettano la costituzione di un mediatore all'interno del Dipartimento di Stato a cui si potrà ricorrere in caso di violazioni sospette o manifeste. E' un altro modo per rispondere a perplessità ed esigenze europee come americane. Le grandi imprese Usa hanno bisogno di questi accordi per poter rimanere sul mercato, visto che le norme comunitarie per la protezione dei dati non consentono il trasferimento dei dati dei cittadini senza che vi sia la garanzia d'una protezione adeguata nel rispetto delle regole della privacy. La novità più importante è però la possibilità di ricorso, finora negata. Le società stesse avranno obbligo di risposta rapida (45 giorni massimo). In caso contrario, un meccanismo di contenzioso sarà accessibile gratis. Secondo il segretario di Stato americano al Commercio, Penny Pritzker, è «un accordo storico», in quanto segna «un punto di svolta» nelle relazioni bilaterali Ue-Usa. Il commissario Ansip ha preferito concentrarsi su quello che resta ancora da fare: «si lavora per garantire che i dati personali dei cittadini siano protetti».


I pm chiudono l'inchiesta Google
Indagati 5 manager per evasione

CORRIERE DELLA SERA
SETTE

Data 04-03-2016
Pagina 23
Foglio 1

Roberto Cotroneo / Blowin' In The Web

La privacy è la vera nemica del sistema

Il mondo virtuale dei *social* funziona soltanto se non è filtrato. A meno di non chiedere di sbloccare un iPhone. Allora si dicono tutti contrari

Il web, e poi i social che a loro modo stanno diventando il web, ci chiede di continuo di formulare domande. Google ha una finestra dove si scrive una frase, si chiede qualcosa, e si attende risposta. Spesso sono soltanto parole allineate che servono a centrare un argomento. Altre volte sono vere e proprie domande che non possono avere alcuna risposta sensata, ma generare un'idea di risposta, che ormai è diventata sinonimo di soluzione. La risposta non è un modo di interloquire ma deve risolvermi il problema. Per cui se chiedo a Google in quale cinema più vicino a casa proiettano il film che voglio andare a vedere e lui mi risponde in modo corretto, ho risolto un problema. Ma se gli chiedo quale autore ha raccontato meglio l'amore in una poesia, la risposta è sempre sbagliata, anche se Google mi dicesse: Catullo. Perché cercare una soluzione dove invece si dovrebbe impostare un dialogo è un errore a cui non si può rimediare.

Da anni si discetta sui pericoli del web e dei social network. Nelle ultime settimane c'è tutto un dibattito se sia corretto pubblicare le foto dei propri figli. E la Rete, come sempre si è spaccata (come se poi fosse mai stata integra e unitaria). Sono problemi importanti, si sa che mostrare i propri figli minori è un azzardo, e sarebbe meglio avere più privacy. Ma al tempo stesso Mark Zuckerberg annuncia al mondo, dal World Mobile Congress che il futuro sarà il video, internet per tutti, le reti sempre più veloci 5G, la realtà virtuale. E così ci si potrà mostrare ancora meglio.

Ma tra le domande a cui Google non sa rispondere c'è naturalmente quella non tanto della frantumazione di tutte le privacy, semmai dell'implosione. La tecnologia ha spostato il suo asse, da strumento per risolvere i problemi ad altoforno che macina e cuoce tutto quello che esiste trasformando la realtà in un'altra cosa, che prima non c'era. Non si tratta di permettere a un nonno islandese di chiacchierare ogni giorno con il nipote in Tasmania come lo avesse nel condominio di fronte al suo. Si tratta di inventare abitudini prima inesistenti.

NON È REALTÀ. Pubblicare le foto della propria famiglia su Facebook, del proprio bimbo nella culla o del sushi appena preparato, non è come mostrare l'album di famiglia agli amici o invitare i parenti a cena ed esibire il piatto con entusiasmo ed orgoglio. È un'altra cosa: è la realtà virtuale. Ed è forse per questo che è ancora complicato convincere la gente a mettere gli occhiali che ti proiettano in un mondo virtuale che sembra vero. E questo per un motivo: che è quello vero a sembrare virtuale, per cui è lì la scommessa del futuro.

Zuckerberg non lo sa. Al punto che si è comprato l'azienda Oculus per inventare una nuova forma di virtualità. I genitori che pubblicano le foto dei loro figli lo sanno bene invece: pensano che viviamo in un mondo che non ha più bisogno di privacy semplicemente perché non è un mondo vero. Come non sono vere le foto dei profili di Facebook anche quando sono vere. Nel senso che scegliere un profilo, un'espressione, un tipo di posa vuole dire già decidere che tipo di inganno identitario si vuole compiere sui social. A meno di non decidere di pubblicare le foto segnaletiche: fronte, profilo destro e profilo sinistro.

In questo mondo virtuale dei social non c'è spazio per la privacy: perché è un inciampo in bianco e nero in un mondo a colori. I social funzionano se non sono filtrati. Se li chiudi non rendono più. E la privacy è nemica del sistema. A meno di non chiedere di sbloccare un iPhone. In quel caso le cose cambiano. Tutti solidali con Apple: da Google a Facebook. «Daresti le chiavi di casa tua a chi te l'ha venduta?», dicono alla Apple. Certo che no. Ma permetteresti a tutta la città di entrare e uscire da quella casa attraverso pareti di vetro, e anche spalancate, che mostrano tutto? A quel punto il portoncino ben chiuso serve davvero a poco. Ma anche questo è marketing. Bello far pensare a tutti che i nostri segreti siano inviolabili persino dall'Fbi quando le Over the Top, ovvero le grandi imprese mondiali che controllano la Rete, hanno reso questo mondo il più violabile e privo di privacy che esista.

CORRIERE DELLA SERA

Data 07-03-2016
Pagina 1
Foglio 1

Allarme sicurezza per l'Anagrafe tributaria

Le indicazioni del Garante per la privacy all'Agenzia delle Entrate e al ministero dell'Economia: «Troppo facile l'accesso di estranei alla dichiarazione dei redditi, inefficaci i sistemi antiabusivi»

Una delle più importanti e delicate banche dati pubbliche, l'anagrafe tributaria, presenta venti «rilevanti criticità» nelle «misure di sicurezza» e nella «qualità dei dati utilizzati per la selezione dei contribuenti ai fini dell'accertamento sintetico»: una sfilza di «vulnerabilità riscontrate» dall'Autorità Garante per la protezione dei dati personali, che le ha segnalate in una lettera sia al direttore dell'Agenzia delle Entrate, Rossella Orlandi, sia al ministro dell'Economia, Pier Carlo Padoan, invitando a «intraprendere nell'immediato ogni sforzo utile a ridurre significativamente i rischi di accessi abusivi, coerentemente a quanto prescritto nel tempo dall'Autorità». Una lettera alla quale l'Agenzia ha risposto tornando a promettere al Garante di porre presto rimedio alla situazione.

Uno di questi rischi riguarda il servizio «Fisconline», nel quale il contribuente può entrare con user name, password, e un Pin di cui riceve online la prima parte, per poi ricevere al proprio domicilio fiscale la seconda parte del Pin e la password in una busta trasmessa dall'Agenzia. Ma le ispezioni del Garante nell'autunno del 2015 hanno rilevato che, se per accedere al «cassetto fiscale» e inviare la dichiarazione dei redditi precompilata è necessaria l'intera procedura di sicurezza rafforzata, il contenuto della sola seconda busta invece già permette, a chiunque ne entri in possesso, di consultare tutti i dati personali sensibili di quel contribuente (a cominciare da quelli sulla salute) contenuti nella dichiarazione.

Poi ci sono le «vulnerabilità» legate all'assenza o inefficacia di sistemi in grado di segnalare accessi potenzialmente anomali («alert») sulla base dello scostamento statistico o comportamentale da parametri standard.

Come sempre in questi casi, occorre trovare un equilibrio tra sicurezza e efficienza della banca dati utilizzata anche da decine di migliaia enti locali e professionisti, altrimenti troppi allarmi equivalgono a nessun allarme e i servizi al cittadino si trasformano in disservizi.

Ma ai tecnici del Garante della privacy, Antonello Soro, la bilancia sembra pendere troppo sull'operatività quotidiana e troppo poco sulla sicurezza: non ci sono «alert» sugli accessi compiuti dai dipendenti dell'Agenzia, mancano persino nel caso di accessi effettuati da utenti che usino «in contemporanea le medesime credenziali», e sono assenti pure «per gli ingressi effettuati dal Centro elaborazione dati delle forze dell'ordine e dagli altri enti con accessi speciali». È capitato addirittura che dalle utenze di alcuni Comuni risultassero «oltre 4.000 accessi a più di 1.000 codici fiscali differenti senza che si innescasse il previsto blocco dell'utenza».

Anche laddove esistono procedure in teoria rassicuranti (come l'obbligo di autorizzazione del superiore gerarchico per il dipendente che voglia consultare l'archivio dei rapporti finanziari), la realtà rivela curiose falle: come il fatto che l'applicativo «Vermont», che raccoglie tutte le tracce (i log) di chi entra nel sistema, accetti però due volte l'inserimento dello stesso codice fiscale. E pure l'obbligo per gli utenti della piattaforma di consultazione «Puntofisco» di scrivere in un campo la motivazione degli ingressi, finalizzato «a facilitare un controllo a posteriori sulla legittimità degli accessi», in pratica è «vanificato» dal fatto che in quel campo basti scrivere persino alcune lettere a casaccio.

Luigi Ferrarella
lferrarella@corriere.it

LA STAMPA

Data 07-03-2016
Pagina 15
Foglio 1

Cyber-ricatti Anche le aziende sotto attacco

Chi non paga rischia di perdere tutti i dati sul computer

La storia

GABRIELE MARTINI
TORINO

Funziona così: ti arriva una mail, apri il documento allegato, passa qualche ora e sul computer ti appare una scritta a tutto schermo: «Se stai leggendo questo messaggio, significa che tutti i tuoi file sono stati bloccati. Per riaverli devi pagare». Di solito svariate centinaia di euro.

Il cyber racket è la diavoleria più in voga tra i criminali informatici. In gergo: "ransomware". Sono virus che criptano i dati di un computer e chiedono un riscatto per renderli nuovamente leggibili dall'utente. Non sfruttano falle informatiche ma l'ingenuità degli internauti. «Sono campagne di estorsione informatica», spiega Paolo Dal Checco, consulente informatico forense dello studio Di.Fo.B. di Torino. «Esistono da 15 anni, ma il salto di qualità avviene nel 2014». E' l'anno del boom del bitcoin: la moneta virtuale favorisce l'anonimato e abbatte i costi di riciclaggio. Spuntano virus sempre più sofisticati. Inizia una rincorsa continua tra guardie e ladri. Quasi sempre vincono i secondi.

Nel mirino

Aziende, piccoli imprenditori, professionisti, privati: l'elenco delle vittime si allunga di giorno in giorno. Soprattutto in Italia. «Ci hanno chiesto 400 euro, cifra per noi irrisoria. Non abbiamo pagato per principio»>, racconta Luca Cotterchio, ad di Ascot ascensori, tra i gruppi leader del settore con 80 dipendenti e fatturato di 10 milioni di euro. «Il virus era in una mail scritta in italiano. I nostri informatici hanno bloccato l'attacco e dopo due giorni di lavoro hanno ripristinato tutti i documenti grazie ai backup». Le imprese sono restie a denunciare il cyber racket. Molte pagano. Un'azienda orafa di Arezzo pochi giorni fa ha versato 3.600 euro. Ma poi gli hacker non hanno sbloccato il computer.

La Revello è un'azienda veronese che commercia prodotti odontoiatrici ha 350 dipendenti e venditori in tutta Italia. «La tecnologia è il nostro punto di forza», spiega Matteo Quagini, capo dell'area informatica. «Abbiamo salvato i server solo perché il sistema ha segnalato l'anomalia e i tecnici hanno subito isolato il computer infetto». Non tutti sono così reattivi. Uno studio di avvocati di Roma ha preferito pagare. Un'azienda di grande distribuzione del Nord Ovest ha ceduto: ripartire dal backup sarebbe stato più costoso. Anche una carpenteria metallica del Nord Est ha sborsato. Il caso estremo, una ditta con una cinquantina di dipendenti in Lombardia: ha pagato ma la richiesta di riscatto era scaduta. Bolle, fatture, contabilità, dati dei clienti: tutto svanito per sempre.

Non è un fenomeno solo italiano. La Hollywood Presbyterian Medical Center, nota clinica di Los Angeles, ha scucito 17 mila dollari per sbloccare Tac, computer e strumenti informatici. Secondo Clusit, l'associazione che riunisce decine di aziende di sicurezza informatica, nel 2015 c'è stata una crescita esponenziale. «Negli ultimi mesi sono stati colpiti anche enti locali come ospedali e Comuni», confermano dalla Polizia postale. Dietro questo boom c'è un fenomeno nuovo: il franchising del racket digitale. Fino a pochi mesi fa, gli attacchi partivano quasi tutti da Est Europa e Russia. Chi creava il virus, tentava di infettare i computer. Poi la strategia dei pirati informatici è cambiata: oggi sfornano software su misura venduti chiavi in mano nel deep web. Spesso per comprarli non servono nemmeno soldi: basta una percentuale sulle future estorsioni. Chi li acquista deve solo scegliere la lingua, decidere quanti bitcoin chiedere come riscatto e lanciare l'amo.

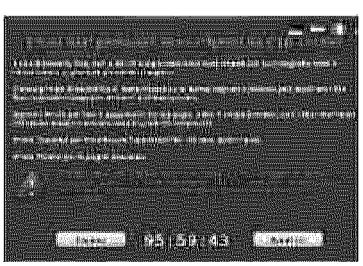
Il cyber racket si diffonde via mail o siti web infetti. D'improvviso il computer si svuota, tutti i contenuti diventano inaccessibili. Pagare conviene? «No, si incentivano le estorsioni», spiega Dal Checco.

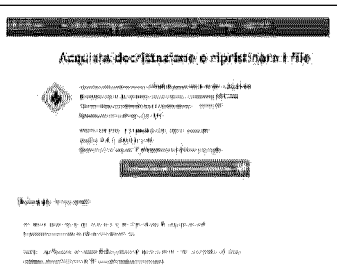
L'organizzazione

«Dietro questi attacchi ci sono organizzazioni criminali che lavorano con programmatori, traduttori e analisti finanziari», spiega Alessio Pennasilico, security evangelist di Obiectivo. «Alcuni offrono persino un "numero verde" da chiamare in caso di difficoltà con i bitcoin. Ci tengono alla loro reputazione». E gli hacker hanno nuovo obiettivo, avverte Pennasilico: «Gli smartphone. Prima o poi cripteranno anche tv, frigo, automobili e pacemaker».

I siti

L'esca Un sito internet truffa usato per diffondere il virus





Il business Sito dove è possibile acquistare il virus in franchising

CORRIERE DELLA SERA

Data 08-03-2016
Pagina 35
Foglio 1

La sicurezza

Botta e risposta sulla privacy Agenzia Entrate-Garante «Ora tutto ok». «Non è vero»

Tutto già risolto nella sicurezza dell'Anagrafe tributaria, giura l'Agenzia delle Entrate. Sorprende che l'Agenzia lo dica quando non è vero, osserva il Garante della privacy. E' botta e risposta dopo la pubblicazione sul *Corriere* delle venti «rilevanti criticità» e «vulnerabilità» nelle «misure di sicurezza» dell'Anagrafe tributaria, denunciate dal Garante in una missiva all'Agenzia diretta da Rossella Orlandi (che aveva risposto con un impegno a mettersi in regola) e al ministro dell'Economia, Pier Carlo Padoan.

All'ora di pranzo l'Agenzia, invano qui interpellata da mercoledì scorso, ieri dirama una nota a singolare firma congiunta tra Agenzia delle Entrate e Commissione parlamentare di vigilanza sull'Anagrafe tributaria, dunque tra controllato e controllore. Vi afferma che «alcune delle criticità sono state già risolte dall'Agenzia attraverso l'adozione di misure correttive introdotte seguendo una valutazione di priorità»: come il fatto che dal 2016 non si dovrebbe ripetere la falla riscontrata nell'autunno 2015 dal Garante, e cioè che la seconda parte del Pin (recapitato per posta) bastasse a chiunque per leggere le dichiarazioni precompilate dei redditi. «Per altri rilievi l'Agenzia ha elaborato un insieme di osservazioni, misure ed adeguamenti già notificati al Garante entro il prescritto fine febbraio», continua la nota dell'Agenzia che conclude: «La Commissione di vigilanza sull'Anagrafe tributaria, afferma il Presidente on. Gian Giacomo Portas, assicurerà come ha sempre fatto il presidio della sicurezza dei dati».

Ma nel pomeriggio è il Garante della privacy, Antonello Soro, a raccontare un'altra storia: «Sorprendono le dichiarazioni secondo le quali, attraverso l'adozione di misure correttive, sarebbero già state risolte dall'Agenzia le numerose ed importanti criticità riguardo a misure tecnologiche ed organizzative che non possono in alcun modo essere sottovalutate», e che sono state «riscontrate rispetto ad alcune prescrizioni formulate dal Garante all'Agenzia addirittura nel 2008». Al punto che, prosegue Soro, «l'Agenzia, senza aver messo in alcun modo in discussione i rilievi che sono stati formulati» dal Garante, «ha manifestato la volontà di provvedere in futuro alla rimozione degli stessi».

Luigi Ferrarella
lferrarella@corriere.it

La vicenda

● Nei giorni scorsi il Garante della Privacy, con una lettera al ministero dell'Economia, ha lanciato l'allarme sulla sicurezza dell'anagrafe tributaria: presenta «rilevanti criticità» nelle «misure di sicurezza» e nella «qualità dei dati utilizzati per la selezione dei contribuenti per l'accertamento sintetico»

● L'Agenzia delle Entrate e la Commissione di Vigilanza sull'Anagrafe tributaria in un comunicato congiunto precisano che «alcune criticità sono già state risolte attraverso l'adozione di misure correttive introdotte seguendo una valutazione di priorità». Poco dopo il Garante ha diffuso un comunicato definendo «sorprendenti» quelle «dichiarazioni»

Antonello Soro, presidente dell'autorità Garante per la protezione dei dati personali dal 19 giugno 2012, anno in cui si è dimesso da deputato


Carige, la battaglia delle cinque liste

IL FOGLIO

Data 09-03-2016
Pagina 8
Foglio 1 / 3

DAMMI LA TUA PASSWORD

Davvero possiamo accettare di perdere la nostra privacy in cambio di maggiore sicurezza? Il caso Apple, il terrorismo, il nuovo Patriot Act e poi il caos grillino. Girotondo di opinioni

Roma. In principio fu il caso Apple vs. Fbi, che si innestava su una polemica già esistente ma ha aperto il dibattito al pubblico. (Per chi non avesse letto i giornali: la società di Cupertino si è rifiutata di aprire l'accesso dell'iPhone del terrorista che uccise 14 persone a San Bernardino adducendo ragioni di privacy e sicurezza, e l'Fbi l'ha trascinata in tribunale). Poi è arrivata la notizia delle spiate dell'americana Nsa a Silvio Berlusconi, sono arrivate le proposte di legge dei governi francese e inglese che aumentano i poteri degli organi d'indagine a scapito della privacy, è arrivato, grazie allo scoop del Foglio, il caso della "spectre" Casaleggio, che ha avuto accesso ai server dei parlamentari grillini, a loro insaputa. Mai come in queste settimane si è parlato di privacy in termini che non riguardano soltanto la salvaguardia dell'intimo dell'individuo, ma anche il suo difficile e forse impossibile equilibrio con le esigenze di sicurezza, libertà, democrazia. Abbiamo sentito alcuni esperti, analisti e uomini delle istituzioni per chiedere loro se questo equilibrio è ancora possibile. Ecco cosa ci hanno detto.

L'Europa rischia di perdere se stessa

Mentre ancora divampa la polemica sul doppio fronte Apple-magistratura statunitense e Nsa-Governo italiano, Obama promulga una legge (Judicial Redress Act) che estende ai cittadini europei alcune garanzie per i trattamenti dei loro dati da parte delle autorità statunitensi. Legge importante, che sottende la consapevolezza dell'impossibilità di discriminare gli utenti di una realtà globale come quella digitale in ragione della nazionalità, come ha chiarito la Corte di giustizia annullando l'accordo sul trasferimento verso gli Usa dei dati dei cittadini europei. Ma resta il double standard previsto dalla riforma dell'intelligence (Freedom Act), che pur introducendo alcune garanzie rispetto alle acquisizioni di dati personali per fini di sicurezza, lascia fuori, in gran parte di tale settore, i non americani. Idea paradossale, quella di limitare ai soli cittadini un diritto che nasce su quel IV emendamento, voluto proprio per contrastare le ingerenze nella vita dei cittadini già praticate, nel XVIII secolo, dal Governo inglese. Un diritto nato per garantire libertà e autonomia non può conoscere confini e discriminazioni per nazionalità. Non a caso, non solo in Europa, esso è considerato diritto fondamentale, come tale da riconoscere alla persona in quanto tale, a prescindere dal requisito della cittadinanza. Se dopo il Datagate gli Usa abbiano compreso il valore reale della protezione dati, soprattutto nel suo rapporto con la sicurezza, è ancora presto a dirsi. Certo è che la risoluzione delle vicende di questi giorni sarà significativa. Lo sarà la definizione del caso Apple, se si ammetterà pure l'accesso al telefono dell'attentatore (con tutte le garanzie estese, dalla Corte suprema, dalla materia della libertà personale a quella della perquisizione di strumenti che così tanto hanno di "personale"), senza però vietare in generale la criptazione. Importante sarà la volontà di accertare davvero, senza trincerarsi dietro il segreto di stato, eventuali responsabilità dell'Nsa per le intercettazioni ai danni del nostro governo, ma anche per le acquisizioni di milioni di dati di cittadini italiani. Dirimente sarà la scelta, più generale e non solo americana, di basare le indagini di polizia, anche antiterrorismo, su controlli mirati e selettivi e non sulla sorveglianza massiva, che oltre a essere democraticamente insostenibile si è anche dimostrata del tutto inefficace. Ma la "costituzionalizzazione" dell'emergenza in Francia e le ripercussioni che l'allarme terrorismo ha avuto da noi, fanno temere che proprio quell'Europa che ha rappresentato un modello verso cui tendere nel rapporto tra libertà e sicurezza, si allontani da se stessa. E da quei princìpi che ne fondano l'identità: la garanzia della privacy soprattutto, come presupposto di libertà e democrazia.

Soro: "La polizia deve basare le sue indagini, anche di antiterrorismo, su controlli mirati e non sulla sorveglianza massiva

Antonello Soro
Presidente dell'Autorità Garante per la protezione dei dati personali

Il dibattito parte da prospettive sbagliate

Definire la polemica intorno a sicurezza e privacy come frutto di una contraddizione è fuori fuoco. Il punto è chiedersi: cos'è la sicurezza? Rispetto anche solo a pochi anni fa, con tutte le tracce digitali che lasciamo, sono a disposizione informazioni sulle persone come mai prima nella storia dell'umanità. Il livello di informazione è altissimo, ma questo non corrisponde a una percezione di un maggiore livello di sicurezza. In questo senso, bisogna riconoscere che il dibattito non è tra privacy e sicurezza, ma tra privacy e raccolta di dati. Il problema è che estrarre informazioni dai dati, utili per ottenere maggiore sicurezza, non è un processo automatico, anzi. Bisogna cercare il classico ago in pagliai sempre più grandi. Si pensi agli attentati del 13 novembre a Parigi: i servizi segreti di molti paesi europei avevano una buona quantità di informazioni sui terroristi, ma non sono riusciti a metterle insieme e a ricavare intelligence adeguata. Non possiamo dire che più informazioni equivalgano a più sicurezza, non c'è una raccolta di dati che possa sopperire a una buona capacità d'intelligence. E tutto questo mentre viviamo in un'epoca d'oro della sorveglianza, in cui mai come oggi i dati delle persone sono a disposizione del pubblico e dei governi. Il caso di San Bernardino è una questione ancora diversa. I ruoli vanno ribaltati: Apple combatte per la sicurezza, non per la privacy. Creare una porta di servizio dei dispositivi (una backdoor) è pericoloso perché non esistono chiavi che funzionano solo per i buoni.

Mori: "Apple non vive in un universo sovranazionale. Non può decidere di fare il padreterno con il destino degli altri"

Si prenda il caso di Juniper Networks, società americana che costruisce apparati di gestione di rete per privati e istituzioni, tra cui istituzioni americane. A dicembre dell'anno scorso Juniper ha scoperto due backdoor nel software dei suoi apparati; alcuni esperti hanno suggerito, senza mai confermare definitivamente, che proprio l'americana Nsa potrebbe essere responsabile indiretta di queste backdoor. E persino il dipartimento della Difesa è stato coinvolto in furti di dati di 21,5 milioni di lavoratori federali e contenenti impronte digitali di 5,6 milioni di persone. Alcuni ritengono che nel suo tentativo di ottenere più informazioni, l'Nsa potrebbe aver involontariamente danneggiato la sicurezza. La discussione attuale nella politica e sui media, dunque, è piuttosto superficiale dal punto di vista tecnico. Il dibattito è molto emotivo, ed è difficile mettere a fuoco il fatto che un aumento della quantità dei dati a disposizione dei servizi non significa necessariamente maggiore sicurezza. Si conti inoltre che è stata l'Fbi a determinare le condizioni per non avere in automatico tutte le informazioni del terrorista di San Bernardino, facendo cambiare ad Apple la password della cloud dell'utente nei primi giorni dopo l'attentato. E' un errore banale, che non ci si aspetterebbe da persone con adeguata formazione e con processi controllati. La sola Apple ha venduto 900 milioni di iPhone. E se un si-

mile errore banale accadesse con le chiavi della loro porta di servizio?

Stefano Quintarelli
deputato del Gruppo misto, e imprenditore nel settore delle telecomunicazioni
(testo raccolto dalla redazione)

La sopravvivenza dello stato prevale sempre

La contraddizione tra sicurezza e privacy è solo apparente. E' possibile uscirne con una constatazione di fatto. Ci sono interessi superiori a quelli di un'azienda privata o di un cittadino, anche se questi vengono presentati come la difesa della riservatezza del cittadino. La sopravvivenza di uno stato e delle istituzioni statali a mio avviso prevale sull'interesse del singolo. Questo vale anche nei casi di terrorismo nazionale o internazionale come quello trattato nella disputa intorno ad Apple, che rappresentano pericoli esiziali per la sicurezza di uno stato.

La privacy è un valore non negoziabile, ma quando diventa una pretesa intransigente si trasforma in un'ipocrisia. C'è un'evidente prevalenza dei valori, che deve essere valutata caso per caso ma non può essere negata. Questa prevalenza dei valori può essere messa in luce da un esempio: nel 1945, all'indomani della fine della Seconda guerra mondiale, gli Stati Uniti erano l'unica potenza a possedere la bomba atomica. Gli scienziati che vi avevano lavorato possedevano segreti che avrebbero messo in pericolo un'intera nazione. In casi come questo, lo stato ha una superiore capacità e potestà d'intervento. Né Apple né nessun altro possono arrogarsi il diritto di gestire a proprio piacimento un segreto che può mettere in pericolo la nazione.

Apple non vive in un universo sovranazionale. Nasce nell'ambito di un'istituzione statuale e a essa deve rispondere. Mantenere il segreto su determinati aspetti legati alla sicurezza nazionale può provocare danni gravissimi alle istituzioni e ai cittadini, e una società privata non può comportarsi come un padreterno decidendo il destino degli altri. Il problema si pone semmai sul lato delle garanzie: chi deve decidere se l'interesse nazionale sovrasta ogni altra esigenza? A mio avviso deve essere l'organo supremo della magistratura, la Corte Suprema per gli Stati Uniti o la Consulta per l'Italia. A partire dal 2013, il cosiddetto scandalo Datagate ha indebolito presso il pubblico la consapevolezza della necessaria prevalenza della ragione di stato, mostrando che i segreti di una nazione possono essere in qualche modo accessibili e propalabili. Ma le informazioni diffuse da Snowden e compagnia non erano nemmeno qualificabili come notizie. I possibili nuovi casi di terrorismo invece lo sono.

Mario Mori
generale, ex comandante del Ros e direttore del Sisde
(testo raccolto dalla redazione)

La privacy è morta e sepolta

Dicono giustamente che per difendere la sicurezza dei cittadini non si può comprimere la libertà e la privacy di nessuno, compresa la libertà d'espressione, ma io sono abbastanza scettico sulla credibilità di queste affermazioni. Sono convinto che la privacy come era intesa anche soltanto vent'anni fa, come garanzia assoluta dell'intimo dell'individuo, sia morta e sepolta da tempo. Personaggi come Kerouac, vagabondi che passano da un luogo all'altro senza essere notati né registrati, oggi non potrebbero più esistere. Il problema ormai non è più preoccuparsi per la violazione della privacy tradizionale, perché il controllo è pressoché totale. Il punto è lo stadio successivo, quello che potremmo definire come privacy di secondo livello, che è l'unica che siamo ancora in tempo a tutelare e che concerne la diffusione degli elementi che emergono dalla violazione della privacy di primo livello. La diffusione comprende naturalmente la pubblicazione attraverso i media, e questo apre il delicatissimo tema della libertà d'espressione, che deve rimanere a tutti i costi sacra, e dell'autoregolamentazione degli organi di stampa.

La morte della privacy è avvenuta anche a causa di un incredibile avanzamento tecnologico. Guardiamo ad esempio al caso di Hacking Team, società italiana leader nella creazione di strumenti di spionaggio. Esso dà idea delle guerre stellari che si stanno combattendo in questo campo, guerre nelle quali noi spesso siamo costretti a difenderci con una manciata di articoli del Codice penale – mi riferisco agli articoli 615ter e seguenti –, spesso inadeguati alla situazione attuale. In un contesto in cui queste violazioni diventeranno sempre più problematiche, bisognerà riconsiderare la notevole offensività di tali reati che attualmente vengono ritenuti, quanto la pena, molto meno gravi di un furto al supermercato. Basti pensare che l'accesso a una banca dati oggi viene punito con un massimo di soli quattro anni di reclusione. L'intervento di Apple in questo dibattito mi sembra ipocrita e rispondente più che altro a logiche di mercato. Il doppio standard della società, che in paesi autoritari come la Cina è piuttosto accondiscendente alle esigenze del governo, mostra che Apple non ha la credibilità per ergersi come vestale della privacy. Smartphone, tablet, webcam, tecnologie di riconoscimento facciale, big data, strumenti di spionaggio informatico come quelli di Hacking Team: in questo mondo parlare di privacy è risibile. Non può essere più controllata al primo livello, quello dell'intimità. E' sul secondo livello, quello della pubblicazione, che dobbiamo lavorare senza pregiudizi e con grande rigore.

Piero Tony
ex procuratore capo di Prato
(testo raccolto dalla redazione)

La riservatezza non è un'idea immutabile

Ancora una volta ci troviamo a dover scegliere tra libertà e sicurezza. Una scelta che, in momenti come questo, è troppo facile orientare verso la sicurezza, ma altrettanto miope e pericoloso. Sarebbe ingenuo pensare alla privacy come concetto immutabile. Un esempio? dobbiamo arrivare alla seconda metà del Settecento perché gli architetti introducano il concetto di corridoio. Prima di allora per andare da un punto all'altro della casa era normale passare attraverso le singole stanze. Stanze nelle quali gli inquilini erano presi dalle loro attività quotidiane: mangiare, dormire, lavarsi. Un stile architettonico che accomunava le case dei villani e quelle dei signori. Madame de Maintenon, raccontano gli storici, dormiva nella stessa stanza in cui suo marito Luigi XIV riceveva i ministri: "mentre il re discute le cameriere la spogliano e l'aiutano ad andare a letto", narrano le cronache. Nulla di strano tutto sommato, se si pensa che pare che il Re Sole fosse aduso ricevere seduto sulla "seggetta".

Quintarelli: "Il livello delle informazioni è già altissimo, ma questo non corrisponde a un maggior senso di sicurezza"

Tuttavia se pensiamo alla privacy come il "diritto di essere lasciati soli", in un mondo in cui esser soli per scelta è sempre più difficile, ci troviamo di fronte a un diritto che non solo va tutelato con tutta la forza di cui siamo capaci, ma rispetto al quale sarebbe pericolosissimo abdicare. E non solo per questioni etiche o di principio, ma anche – nel caso della disputa tra Fbi e Apple – per mere ragioni di convenienza. Che succederebbe se esistesse uno strumento in grado di leggere qualsiasi contenuto riservato presente in un device? E che succederebbe se questo strumento finisse nelle sbagliate? O, ancora peggio, chi determina quali siano le mani sbagliate? Quale sarebbe il danno – in termini di sicurezza – se ad essere aperti non fossero i cellulari "dei cattivi", ammesso che sia sempre possibile stabilire chi sia il cattivo? Insomma: per "aprire" i contenuti di un singolo device è necessario disporre di uno strumento in grado di aprirli in qualsiasi device. E avere questo strumento, oltre a rappresentare una sconfitta in termini ideali, è un rischio che non possiamo permetterci.

Stefano Epifani
professore di Social media management all'Università La Sapienza di Roma

Perché serve un Patriot Act

Non bisogna ovviamente rinunciare alle libertà pubbliche e alla protezione della privacy, ma detto questo, in ogni tipo società, il grado di sicurezza dipende dalla quantità di libertà che si è disposti a sacrificare: più libertà sacrificata equivale a più

sicurezza, e viceversa. Tutto sta nel capire dove poniamo il cursore tra la libertà e la sicurezza, e questo è il principale problema dei politici. Bisogna però essere tutti consapevoli che non potremo mai avere il 100 per cento di sicurezza se non rinunciamo a una parte della nostra libertà. Alle molte personalità e associazioni che hanno gridato allo scandalo e parlato con toni dispregiativi di "Patriot Act alla francese" a proposito della legge sulla sorveglianza digitale e sui servizi segreti promulgata lo scorso luglio, va detto che era necessaria per far fronte alla crescente minaccia terroristica. Ma iscrivere nella Costituzione lo stato d'emergenza, come è stato fatto dal governo socialista di Parigi, non ha nessuno senso, perché lo stato d'emergenza esiste già nella legge francese, basta applicarlo. La maggior parte dei problemi che abbiamo avuto in questi ultimi anni in materia di terrorismo sono dovuti al fatto che in Francia applichiamo molto male le nostre leggi. Dando invece uno sguardo a ciò che è successo di recente negli Stati Uniti, mi chiedo: come può Apple ergersi a paladina della privacy quando quotidianamente, alla stregua di tutti gli altri giganti della telefonia e di internet, non si fa scrupoli nel trasmettere ogni sorta di dati a delle società commerciali per fini pubblicitari? Se l'Fbi ha delle buone ragioni per decrittare il telefonino di una persona che ha partecipato a un attentato terroristico, deve poterlo fare. Naturalmente sotto il controllo del giudice.

Tony: "Non possiamo più difendere la privacy come la conoscevamo vent'anni fa. Il problema è la diffusione"

Alain Chouet
ex agente dei servizi segreti francesi ed esperto di antiterrorismo
(testo raccolto dalla redazione)

Più difficile difendersi dagli attacchi

La contraddizione tra sicurezza e privacy è al centro di un dibattito pubblico che si sta sviluppando soprattutto negli Stati Uniti, grazie alla presenza di importanti attori nel campo tecnologico (come Microsoft, Apple, Facebook, Twitter etc.), attori istituzionali come Cia, Fbi e Nsa, nonché e una certa maturità di parte dell'opinione pubblica in materia di sicurezza cibernetica, privacy e crittografia. I rischi sono evidenti, e per enumerarli bisogna partire da un discorso di fondo. Le organizzazioni terroristiche hanno cominciato già da tempo a usare strumenti tecnologici per le loro attività: comando e controllo, reclutamento, finanziamento. Lo Stato islamico e la sua attività online ne sono un esempio lampante. E' chiaro che sono in atto alcune evoluzioni tecnologiche che stanno rendendo sempre più complesso il lavoro delle agenzie di law enforcement. Infatti, l'impiego di determinati strumenti tecnologici in grado di rendere sicure le nostre comunicazioni rischia di rendere inaccessibili informazioni vitali per le attività di prevenzione o indagine. Il dilemma fra privacy e sicurezza, se non affrontato attraverso politiche adeguate in grado di tenere in considerazione anche gli aspetti tecnologici, rischia di indebolire tanto le nostre capacità di difenderci da attacchi cibernetici, quanto di rendere i nostri dati non protetti. Su queste questioni il dibattito in Italia è quasi nullo, eccezion fatta per l'interesse di pochissimi tecnici o di una cerchia ristretta di esperti. La questione non riguarda solo il terrorismo internazionale o nazionale. Il cosiddetto cyberwarfare, cioè la capacità di attaccare gli stati usando strumenti informatici o di difendersi dagli stessi, rischia di essere influenzato dai risultati del dibattito sulla privacy.

Tommaso De Zan
ricercatore presso il programma Sicurezza e Difesa dello Iai
(testo raccolto dalla redazione)

(a cura di Eugenio Cau. Ha collaborato Mauro Zanon)

CORRIERE DELLA SERA

Data 14-03-2016
Pagina 37
Foglio 1

Particelle elementari

di **Pierluigi Battista**

Privacy, forza Apple contro gli Stati intrusivi

Lo Stato è un «mostro freddo», diceva Max Weber, dall'appetito insaziabile. Non vuole argini che limitino la sua onnipotenza: sono le democrazie liberali che ne contengono la smania di controllare tutto, intromettersi ovunque, ficcare il naso in ogni atomo della vita dei cittadini che reclamano il diritto inalienabile a una sfera privata sottratta ai tentacoli dello Stato. Perciò chi ha a cuore l'integrità di una sfera privata, o di ciò che resta oramai di una sfera privata già ridotta al pallido simulacro di se stessa, non può che tifare per la Apple che si rifiuta di consegnare allo Stato americano le chiavi per irrompere nella vita dei cittadini, e spiarla senza limiti. Dicono: non è vero, gli inquirenti americani non vogliono intromettersi nella vita delle persone, non siate paranoici. Sbagliato: la forza del potere politico deve essere contenuta per evitare che dilaghi l'arbitrio, non c'entra la buona fede di chi in un momento specifico la esercita. Dicono: ma senza quelle chiavi non possiamo usare un'arma formidabile per scovare degli assassini. Sbagliato: con questo ragionamento perché non permettere la tortura per estorcere confessioni utili contro assassini reali i potenziali? O non procedere a rastrellamenti di massa, ad arresti senza mandato? Non potremmo avvalerci di strumenti efficaci per neutralizzare ladri e criminali, mafiosi e terroristi? Dicono: allora niente intelligence per la cattura di assassini senza scrupolo. Sbagliato: i servizi segreti si chiamano segreti per un motivo preciso, hanno un campo circoscritto di azione, non pretendono di diventare legge generale. Lo Stato, poi, esibisce sempre buoni propositi e nobili intenzioni, per appagare la sua smania di controllo. Con la scusa della lotta all'evasione fiscale, sta abolendo ogni segreto sui nostri conti bancari, sui nostri movimenti al bancomat, persino sugli spiccioli. Dicono: ma se non hai niente da nascondere di cosa hai paura? Sbagliato: il diritto alla riservatezza non è sinonimo di criminalità. E il mito dell'assoluta trasparenza è una mostruosità totalitaria, indice di una perversa mentalità autoritaria. Nel suo romanzo *Il palazzo dei sogni* subito censurato dalle autorità comuniste albanesi, Ismail Kadaré, che ha ben conosciuto gli orrori del totalitarismo, ha descritto uno Stato che pretendeva di controllare persino ciò che le persone vedono nel sonno. È l'aspirazione segreta di ogni Stato i cui poteri non siano temperati e arginati. Forza Apple.

CORRIERE ECONOMIA

Data 14-03-2016
Pagina 20
Foglio 1

L'analisi

Privacy e dati personali, il diritto di negoziarli

Le tesi nel libro del commissario dell'Agcom Antonio Nicita

DI **EDOARDO SEGANTINI**

Antonio Nicita, l'economista che ha sostituito il dimissionario Maurizio Dècina nel consiglio dell'Authority per le Comunicazioni (Agcom), ha raccolto le riflessioni scritte in questi anni sui principali temi dell'economia digitale. E ora le propone in un libro sotto forma di domande. Quattro capitoli: consumatori e concorrenza, reti e innovazione digitale, pluralismo e media, ecosistema elettronico e diritti.

Due riflessioni, in particolare, colpiscono. La prima riguarda il cosiddetto «capitalismo dei dati», di cui sono sovrani i grandi gruppi di Internet, e che si basa sulla «profilazione» degli utenti. Ovvero il trattamento delle informazioni personali, che servono a moltiplicare l'efficacia del marketing. La «pubblicità aumentata».

«Mi chiedo — scrive Nicita — se non sia il caso di andare oltre la tutela della privacy e non si debba invece guardare al diritto del consumatore a contrattare la propria profilazione e, dunque, a valorizzare il suo potere negoziale al fine di condividere i guadagni derivanti dal "prodotto". Perché in rete il prodotto siamo noi».

In altre parole: se è vero che i dati hanno un valore, un altissimo valore che fa la ricchezza degli Over the Top, è giusto che l'utente sia messo in condizione di vincolarli, oltre che al rispetto della riservatezza, al suo diritto di ricavarne una quota di profitto. In apparenza un'utopia.

In realtà è una posizione coerente con le nuove tendenze dell'Antitrust europeo, che recentemente ha messo sotto indagine l'accesso ai dati profilati.

La seconda riflessione interessante è la critica a quello che Nicita definisce «broadband-scetticismo». Dietro il quale il commissario Agcom vede «l'elogio dello status quo» e «la difesa eroica, ma velleitaria, di rendite destinate comunque, presto o tardi, a evaporare».

Si può aggiungere questo: dalla qualità dell'infrastruttura a banda larga dipendono la soddisfazione degli utenti, ma anche l'evoluzione dell'informatica nelle imprese.

Lo sviluppo dell'Ict infatti non passa più solo attraverso le crescenti prestazioni hardware del singolo computer, ma soprattutto attraverso l'evoluzione dei software (vedi il programma di AlphaGo, che ha sconfitto il campione coreano di go Lee Sedol), e lo sviluppo del *cloud computing*, cioè le reti di data center che forniscono i servizi su Internet.

A ben vedere, le due riflessioni sono connesse. La crescita dell'economia digitale è legata allo sviluppo della rete, ma i suoi costi e profitti, oggi fortemente sbilanciati a favore degli Over the Top, vanno redistribuiti a vantaggio degli utenti.

Senza dimenticare la necessità di creare diritti e doveri uguali per tutti: big della rete e operatori di telecomunicazioni. Altrimenti lo scetticismo a banda larga non potrà che aumentare e fare danni.

@SegantiniE

edoardosegantini2@gmail.com

metro MILANO

Data 14-03-2016
Pagina 4
Foglio 1

ANTONELLO SORO

SICUREZZA E PRIVACY DIRITTI EQUIVALENTI

Esce oggi in libreria "Liberi e connessi", scritto dal presidente dell'Autorità garante dei dati personali. "Rispettiamo la dignità delle persone"

INTERVISTA «Siamo più a rischio di vent'anni fa, quando la legge sulla Privacy fu concepita. Le regole si sono evolute, certo, ma lo scenario circostante è cambiato più in fretta di quanto potessimo immaginare allora. La consapevolezza che oggi la digitalizzazione della vita espone la riservatezza delle relazioni a grandi sollecitazioni è molto meno forte di quanto lo fosse nel 1996 il bisogno di preservare noi stessi, le informazioni che ci riguardavano, la nostra libertà».

Antonello Soro – medico, già sindaco di Nuoro, a lungo parlamentare, da quattro anni presidente dell'Autorità garante dei dati personali – manderà oggi in libreria per Codice Edizioni "Liberi e connessi", un libro destinato a fare giurisprudenza in tema di privacy e Internet.

Presidente Soro, davvero la società della condivisione, quella in cui viviamo, è così poco consapevole delle dinamiche che la regolano?

Il livello di conoscenza delle opportunità che il digitale ci offre è molto alto. Meno quello dei rischi a cui ci espone. Non tutti hanno compreso quanto un messaggio su Whatsapp, un acquisto on line, una chat su Facebook sono piccoli atti singoli, che possono apparire come insignificanti tessere di un mosaico, ma che qualcuno ha invece interesse a completare. Per produrre un profilo, per conoscerlo e magari condizionarlo, per utilizzarlo commercialmente.

In gioco c'è la riservatezza delle nostre azioni

Di più. In gioco c'è la nostra libertà. La nostra vita si svolge sempre più nella dimensione digitale e non possiamo rischiare di delegare alle tecnologie il nostro potere di scegliere liberamente, ma rivendicare la nostra identità e non subire quella costruita dai profili che altri hanno disegnato per noi. Lo dobbiamo sapere per utilizzare noi la Rete e non viceversa. Di questo parlo nel mio libro.

Ma la tracciabilità delle nostre azioni aumenta la trasparenza. Questo vale per il singolo cittadino, come per le istituzioni. E questo è un bene, un valore. O no?

Certo che lo è, ci mancherebbe. La vita democratica si basa sulla trasparenza delle singole azioni. Ma quelle tracce devono poter essere tutelate. Il tema di oggi è questo. Il diritto alla riservatezza non è un diritto di rango inferiore a quello all'informazione o alla sicurezza, persino alla dignità dell'individuo. Sono diritti paritari in una società democratica. Trovare un equilibrio non è sempre facile, prenda le cronache giornalistiche delle ultime settimane sul caso Regeni o sull'omicidio Varani.

I media hanno esagerato? Perché?

Beh, nel racconto delle torture o dei dettagli dei due omicidi in questione il confine tra la corretta informazione e il rispetto della dignità della persona, in questo caso una vittima, non è stato rispettato. Lo ripeto: il diritto di una società ad essere informata e quello di un individuo a veder tutelata la propria sfera più intima (pensi al dolore delle famiglie) sono diritti equivalenti. Non ce ne è uno prevalente o prioritario. Sulle sevizie a Varani oggi sappiamo particolari eccessivi, forse, e questa conoscenza accentua il dolore di famiglie e persone.

Soliti giornalisti superficiali e famelici?

Io credo molto nell'autodisciplina dei giornalisti, nella forza del loro codice deontologico. E dico che questa riflessione sul bilanciamento tra diritti e doveri non deve mai fermarsi. Un giornalista deve rispettare il diritto del pubblico a essere informato, ma anche quello del singolo ad essere tutelato. Soprattutto se è un singolo debole, non personaggio pubblico.

Apple contro Fbi sui codici criptati di un Iphone, un caso mondiale. Lei con chi sta?

La criptatura di un telefonino è una garanzia fondamentale per tutti. Ma credo che Apple avrebbe potuto aiutare l'Fbi nelle indagini sul killer di San Bernardino senza intaccare la fiducia degli utenti riguardo alla riservatezza delle loro informazioni personali.

Dunque la posizione di Tom Cook è stata un'operazione di marketing?

Dico che l'interesse di Apple a consolidare la fiducia del proprio pubblico è prevalso sul buon senso.

GIAMPAOLO ROIDI

Il Sole 24 ORE

Data 23-03-2016
Pagina 40
Foglio 1

INTERVENTO

Web intelligence contro privacy: regole da definire

di **Andrea Barchiesi**

In un'epoca in cui gli strumenti di **web intelligence** sono diventati sempre più precisi, crescono i timori per la **privacy** e il valore che le si conferisce. Uno scenario conflittuale che cela interessi istituzionali, politici e commerciali.

Il governo Usa ha chiesto supporto ai giganti della Silicon Valley, che dispongono di miliardi di dati di utenti nel mondo, nelle azioni di web intelligence finalizzate alla lotta alla criminalità e al terrorismo. Una richiesta caduta quasi sempre nel vuoto.

Ha fatto discutere il diniego di Apple verso l'ordine di un giudice federale di sbloccare il telefono utilizzato da uno dei sospetti responsabili della strage di San Bernardino che aveva causato 14 vittime. Dopo Apple anche altre aziende hanno affrontato e preso posizione sul tema della privacy e della sicurezza dei dati, ma in assenza di una regolamentazione chiara e condivisa a livello globale, ognuna ha agito orientata dal proprio sentire. Così, da un lato Facebook si è schierata insieme a Google al fianco di Apple, dall'altro ha concesso i propri server ai magistrati che indagano sulla latitanza del boss mafioso Matteo Messina Denaro. Mentre Blackbarry ha subito concesso informazioni su soggetti indagati per narcotraffico alla magistratura torinese.

Uno scenario in cui ciascuno sembra improvvisare, grazie anche all'assenza di un codice che ponga regole e limiti. La posizione di Apple è chiara: in primis la tutela dei consumatori e l'inviolabilità del proprio sistema. Quello che l'azienda tende a difendere è in realtà l'immagine di un sistema inviolabile, più che un diritto. Rifiutare la richiesta dell'Fbi è una posizione scomoda, ma coerente con il modello commerciale, come ha sottolineato l'ad Tim Cook nel suo messaggio. E a sostegno dell'azienda creata da Steve Jobs, nei giorni scorsi è scesa in campo anche l'Onu. Il contesto in cui Apple si muove è comunque una palude, si trattava di scegliere una via o l'altra. E l'azienda di Cupertino ha scelto quella commerciale.

A questo punto è però necessario chiedersi quale sia il limite: di fronte al rischio concreto per la sicurezza delle persone, le aziende hanno ancora la licenza di anteporre il proprio interesse commerciale, scontrandosi con l'opinione pubblica e soprattutto mettendo a rischio la sicurezza dei cittadini/consumatori? D'altro canto è anche opportuno chiedersi come le istituzioni stiano concretamente utilizzando le tecnologie a disposizione per supportare le attività investigative, o quali sono le procedure di web intelligence messe in atto dai governi in chiave antiterrorismo. La Rete è piena di account, pagine, gruppi e community di ogni genere, dal carattere quanto meno borderline. Come viene utilizzato e soprattutto analizzato e monitorato tutto questo materiale dalle istituzioni? Esistono procedure strutturate e meccanismi di alert preventivo quando si rilevano situazioni di questo tipo? Leggiamo spesso di attentati rivendicati da account Twitter o da una pagina Facebook, per poi scoprire che quei profili esistevano da tempo e avevano migliaia di seguaci. L'utilizzo della web intelligence come strumento di monitoraggio preventivo è ancora troppo poco radicato, poco strutturato e spesso utilizzato in modo casuale e tardivo. Tutto ciò rende evidente la necessità di una normativa in grado di stabilire come un'azienda debba comportarsi in questi o simili casi. Per non lasciare che la palude rimanga tale, e per dare regole certe e condivise. E il problema è proprio questo: oggi ci sono giurisdizioni nazionali che di fronte a sistemi e problemi globali non offrono soluzioni e, anzi, rappresentano un limite strutturale della nostra società. Una dimostrazione, questa, di come la legge cerchi di inseguire la tecnologia e i cambiamenti della società. Ma al momento, la legge sembra essere tremendamente indietro.


Ricollocamento, prova al datore

Per il rinvio deposito telematico

Web intelligence contro privacy: regole da definire

DOPO UN ANNO È TEMPO DI BILANCI.

"PRIVACY & SICUREZZA, BINOMIO POSSIBILE: LA SOLUZIONE E' CULTURALE"

L'ANALISI

Dopo le stragi in Francia e Belgio assistiamo a un dibattito disordinato e confuso. Si può trovare la quadra per garantire, al contempo, tutela dei dati e protezione delle persone. Ma i governi devono lanciare campagne di sensibilizzazione sul tema. L'analisi dell'avvocato Guido Scorza

di Guido Scorza, avv. esperto in Diritto Internet

La strage dell'altro ieri di Bruxelles ha riacceso un dibattito al quale abbiamo già assistito all'indomani delle stragi di Charlie Hebdo prima e del Bataclan poi, un dibattito che ruota sempre attorno alla stessa domanda proposta, quasi si tratti di un presupposto ineludibile e del punto di partenza necessario di qualsiasi ragionamento sul tema: è giusto rinunciare ad un po' nella nostra privacy per garantirci maggiore sicurezza?

In Francia il Ministro dell'Interno, Bernard Cazeneuve, si è affrettato a dichiarare, in diretta televisiva, che il suo Governo sta valutando con attenzione l'idea di utilizzare in tutti gli aeroporti tecnologie di riconoscimento facciale per l'identificazione di eventuali terroristi e da più parti, in giro per l'Europa, si è tornati a chiedere a gran voce di rafforzare e centralizzare l'attività di cyber-intelligence anche a costo di chiedere ai singoli Paesi ed ai loro cittadini di rinunciare ad una porzione più o meno rilevante della propria sovranità e del proprio diritto alla privacy.

Vale la pena dire subito senza esitazioni né ambiguità che è un dibattito scomposto, disordinato e confuso che rischia di produrre effetti e conseguenze di matrice culturale, sociale, politica ed economica straordinariamente gravi.

E' ovvio, infatti, che alla domanda se siano o meno disponibili a vivere una vita meno riservata di quella attuale ma più sicura, la quasi totalità dei cittadini europei oe e non solo oe oggi, con le immagini di sangue, dolore e disperazione rimbalzate da Parigi e Bruxelles ancora scolpite nella mente e nell'anima, risponderebbe in maniera affermativa.

E però, per questa via, si propone oe ed anzi si da quasi per scontato oe un rapporto di antiteticità tra due diritti e libertà fondamentali che, nella realtà, non esiste o, almeno, non dovrebbe esistere.

Sicurezza e privacy sono, al contrario, due facce della stessa medaglia, due dimensioni diverse di tutela dell'identità della persona, due diritti e due libertà che competono ad ogni cittadino senza che si debba trovare di fronte all'alternativa di scegliere di inseguirne una, rinunciando all'altra.

A costo di apparire scontati val la pena ricordare le parole di Benjamin Franklin: "Chi è pronto a dar via le proprie libertà fondamentali per comprarsi briciole di temporanea sicurezza, non merita né la libertà né la sicurezza".

Il compito di garantirle entrambe, al maggior livello di intensità disponibile compete naturalmente ai Governi.

Anche perché non c'è alcun dubbio oe e non deve esservi oe che non esiste alcuna proporzionalità aritmetica diretta tra l'aumento della sicurezza e la diminuzione della privacy. La strage dell'altro giorno all'aeroporto di Bruxelles rappresenta la più drammatica e plastica conferma di questa conclusione. E', infatti, difficile immaginare, oggi, in Europa un luogo nel quale il diritto alla privacy sia più compresso e limitato di quanto accada nell'aeroporto di un Paese malauguratamente diventato oe ben prima dell'attentato di ieri oe epicentro noto del sisma terroristico che, da tempo, minaccia l'intero vecchio continente.

Eppure, purtroppo oe forse neppure per caso oe è proprio in quel luogo che i terroristi hanno scelto di portare, ancora una volta, la morte. "Il Belgio conosceva i kamikaze", titola oggi La Repubblica. Un titolo forte, un j'accuse all'indirizzo del sistema di sicurezza ed

intelligence belga ma, più in generale europeo che, però, veicola un messaggio che andrebbe ricordato la prossima volta che qualcuno suggerirà che per garantire ai cittadini europei più sicurezza bisogna che questi ultimi accettino di rinunciare ad un po' della loro privacy.
La sicurezza non è funzione della maggiore quantità di dati che si raccolgono e della minore privacy che si garantisce ai cittadini ma della capacità di analisi e condivisione dei dati dei quali le pubbliche Autorità sono già in possesso. Più sicurezza, dunque, non significa meno privacy.
C'è poi un altro aspetto, egualmente ricorrente, del dibattito che torna a riaccendersi all'indomani di ogni tragedia come quella di Bruxelles. Servono più cybersecurity e cyberintelligence oe si dice da più parte oe e per garantirle bisogna che i cittadini europei accettino l'idea che i loro dati personali in transito attraverso le reti ed i servizi di comunicazione elettronica o, semplicemente, conservati nei loro PC siano più penetrabili ad occhi ed orecchie digitali delle forze dell'ordine.
Ed è per questa strada che nell'ordinamento francese, all'indomani della strage del Bataclan, il Governo si è dotato di poteri straordinari in termini di compressione della privacy digitale dei propri cittadini oe e non solo oe e che la Gran Bretagna si avvia a fare altrettanto mentre la stessa Italia, nicchia e tergiversa ma non disapprova e, anzi, talvolta "accarezza" l'idea di seguire l'esempio.
Quando si parla del rapporto tra privacy e sicurezza nella dimensione digitale, tuttavia, alle considerazioni fatte sin qui, occorre aggiungerne un'altra di straordinaria importanza perché in questo caso, il problema non è solo l'errore che si commette quando si "contrabbanda" per necessariamente alternativo il rapporto tra due diritti e libertà fondamentali.
In questo caso, purtroppo, si fa leva anche su una diffusa debolezza culturale e su una pericolosa sottovalutazione del significato, dell'importanza e della centralità nella vita di un uomo di questa epoca della proiezione digitale della sua identità personale.
Nel 2010, l'allora Ministro dell'Interno Roberto Maroni propose di installare body scanner in tutti i principali aeroporti e stazioni italiani. In tanti, davanti all'idea di doversi ritrovare "nudi" sotto un body scanner per prendere un treno o un aereo manifestarono, forte, il loro dissenso e richiamarono l'attenzione sulla palese sproporzionalità dell'iniziativa specie in assenza di qualsivoglia certezza scientifica oe anche solo su base statistica oe del ricorso a tali strumenti per abbattere la minaccia terroristica.
Oggi, al contrario poiché ci si chiede "solo" di accettare l'idea che Governi e forze dell'ordine possano entrare nei nostri dispositivi mobili e nei nostri PC o accumulare quantità enormi di dati personali, le reazioni appaiono decisamente più tiepide, quasi che la nostra privacy nella dimensione telematica valga di meno di quanto vale in quella fisica.
Si tratta, naturalmente, di un errore di prospettiva figlio dei tempi: il valore dell'immateriale che si tratti della proprietà intellettuale o del nostro diritto alla privacy nella dimensione digitale è, sfortunatamente, ancora percepito oe per ragioni tutte culturali oe come meno rilevante rispetto al valore del materiale.
Ci si sente più violati nella propria privacy nell'essere costretti a passare per uno scanner che ci metta fisicamente a nudo piuttosto che nel sapere che occhi ed orecchie digitali, più o meno indiscrete, scandaglino i nostri PC, tablet e smartphone.
In un contesto di questo genere è compito dei Governi promuovere un processo di educazione alla cultura della privacy all'esito del quale solo sarà possibile "chiedere" ai cittadini di esprimersi in modo consapevole circa la loro effettiva disponibilità a rinunciare oe ammesso che ciò sia davvero necessario oe ad un po' della propria privacy in nome di una semplice, non provata e non provabile ambizione di maggior sicurezza.

il Fatto Quotidiano
NON RICEVE ALCUN FINANZIAMENTO PUBBLICO

Data 25-03-2016
Pagina 7
Foglio 1 / 2

L'ANALISI Il pendolo tra sicurezza e privacy

Ue, nuove misure anti-terrore destinate a impantanarsi

Al summit i ministri assicurano informazioni condivise e più controlli alle frontiere. Come dopo ogni attentato

» STEFANO FELTRI

Come dopo ogni attentato, arriva il momento degli annunci. Al vertice straordinario dei ministri degli Interni e della Giustizia, l'italiano Angelino Alfano propone un "piano nazionale anti-radicalizzazione". Mentre chi si occupa di intelligence e terrorismo si chiede che cosa sia "l'unione di sicurezza" che ha annunciato il presidente della Commissione, Jean Claude Juncker. I contenuti sono vaghi, ma il premier italiano Matteo Renzi è con lui.

I ministri hanno promesso di rafforzare i controlli sui materiali che possono diventare ingredienti per esplosivi, visto che tutte le bombe degli attentati recenti erano artigianali. E poi maggiori controlli ai bordi dell'area di Schengen all'interno della quale c'è la libera circolazione e soprattutto una lunga lista di impegni sulle banche date digitali che dovrebbero permettere di individuare i terroristi prima che colpiscano. Ma che non funzionano o non comunicano tra loro. Una lista di impegni già sentita.

DOPO GLI ATTENTATI alla metropolitana di Madrid viene approvata la direttiva sulla *data retention*, cioè la conservazione dei dati di traffico telefonico e telematico. Con pochi risultati perché ogni Paese la applica a modo suo (Germania e Belgio cercano di sottrarsi a lungo). Nel 2015 la direttiva viene smontata dalla Corte di giustizia europea che ha affermato il diritto alla protezione dei dati personali.

Il principio ribadito dalla Corte è quello che rende molto complesso intervenire in queste materie, perché le limitazioni della privacy devono rispettare vincoli di "necessità e appropriatezza". Cioè essere giustificate dalla gravità dei crimini che vogliono contrastare e non essere ispirate all'approccio della pesca a strascico.

LA TENSIONE tra sicurezza e privacy ha bloccato anche la direttiva sul Pnr (*Passenger name record*), cioè la raccolta delle informazioni sugli spostamenti aerei. Oggi, ogni Paese segue regole diverse nel raccogliere questi dati. Dal 2011, le istituzioni europee cercano di costruire un quadro comune per rendere queste informazioni utili nella prevenzione del terrorismo. Senza successo. Tra i Paesi che più si oppongono c'è proprio la Francia che, dopo la strage di Parigi del 13 novembre, ribalta la sua linea e sostiene ogni accentramento di informazioni.

La proposta della Commissione viene emendata dal Consiglio – cioè i governi – poi arriva nell'Europarlamento dove si arena. Un vasto schieramento, guidato dai Liberali di Alde, pone una questione di principio: la condivisione di informazioni sensibili per la sicurezza deve andare di pari passo all'approvazione delle norme che garantiscono la *data protection*, la protezione dei dati personali, esigenza molto avvertita soprattutto in Germania dove è ancora fresco il ricordo dello spionaggio sui cittadini della parte Est del Paese e ancora più recenti sono le polemiche per la Nsa americana che monitorava il cellulare di Angela Merkel. Da un lato si chiede di raccogliere più informazioni, dall'altro di garantire la privacy.

Dopo gli attacchi al Bataclan, a Parigi, il pendolo si è spostato verso la sicurezza. E così a dicembre la commissione Libertà civili ha dato parere favorevole alla direttiva Pnr, mentre la Commissione avviava l'iter legislativo di una "direttiva terrorismo" che vuole rendere penalmente perseguibili nei Paesi dell'Unione anche tutti gli atti preparatori di un attentato (reclutamento, raccolta fondi, ecc.)

PASSATA L'EMOZIONE di Parigi, però, il 7 marzo il Parlamento ha di nuovo bloccato la direttiva sulle informazioni. Gli inglesi e ora anche i francesi – di tutti gli schieramenti – la vogliono, ma tedeschi, socialisti e liberali frenano. Secondo il coordinatore anti-terrorismo Gilles de Kerchove è uno strumento importante nella prevenzione di altri attentati. E nella riunione di ieri i ministri della Giustizia e dell'Interno hanno preso l'impegno di approvare la direttiva entro aprile. Ma molti deputati e perfino alcuni *think tank* non certo euroscettici come il Ceps, *Centre for European Policy Studies*, sollevano dubbi: raccogliere dati sui passeggeri dovrebbe servire a identificare potenziali terroristi ancora scono-

il Fatto Quotidiano
NON RICEVE ALCUN FINANZIAMENTO PUBBLICO

Data 25-03-2016
Pagina 7
Foglio 2 / 2

sciuti. Ma molti dei membri della cellula che ha colpito a Parigi e poi in Belgio erano ben noti ai servizi segreti di mezza Europa e non solo. E finora la costruzione di grandi *database* digitali nella speranza che lì ci siano i segreti dell'antiterrorismo ha portato a poco, visto che i registri delle impronte digitali non comunicano con il sistema informativo di Europol (l'agenzia che coordina le forze di sicurezza) che a sua volta è sconnesso dal monitoraggio degli accessi nell'area Schengen e così via.


L'ANALISI Il pericolo tra sicurezza e privacy
Ue, nuove misure anti-terrore destinate a impantanarsi

ItaliaOggi

Data 25-03-2016
Pagina 2
Foglio 1

IL PUNTO

Apple non faccia la smorfiosa, è lei una violatrice di privacy

DI SERGIO LUCIANO

C'è qualcosa di stupefacente in questa ormai stiracchiata vicenda dello scontro tra Fbi e Apple sulla decrittazione dei messaggi e degli altri contenuti dell'iPhone del killer di San Bernardino che l'azienda della mela rifiuta di fornire alla polizia di stato americana. È stupefacente e paradossale, perché sembra che in questo scontro la Apple sia la paladina della privacy e i detective siano i fetentoni che vogliono ficcare il naso nella vita privata degli americani. In realtà è vero l'esatto contrario, cioè che le grandi aziende di internet sanno tutto di tutti, e ne approfittano per fare soldi; e i detective di stato, solitamente, e non certo solo negli Usa, elemosinano brandelli di informazioni a caro prezzo tramite hacker ad alto rischio di bufala.

Nella migliore tradizione americana, l'Fbi si è infatti cercata circuiti alternativi per arrivare alle informazioni che le servono, così come fece quando assunse Jack Abbagnale (nessuna parentela con i canottieri olimpionici) cioè il più grande truffatore di tutti i tempi, per metterlo a capo della divisione antitruffe.

Ma resta il tema profondo dello scontro: la Apple è sincera quando difende la privacy dei suoi clienti, anche a costo di contrastare la Fbi? Forse sì, o almeno lo è il suo attuale capo, Tim Cook. Ma nella sua essenza la Apple, come Google, come Facebook, vive di violazioni della privacy. Proviamo a spiegarci.

I dati personali di tutti noi, dalla nostra identità ai nostri gusti, alle nostre opinioni, dovrebbero essere, per l'appunto, personali, cioè mai a disposizione di scopi commerciali, se non dietro autorizzazione esplicita «di volta in volta». E dovrebbero invece sempre essere a disposizione delle autorità, quindi anche dell'Fbi, in casi di forza maggiore e di interesse superiore. Invece i big di internet guadagnano appunto sfruttando i dati che noi lasciamo loro, e si sa che Apple è pienamente annoverabile in questo gruppo, perché pur producendo anche oggetti gestisce soprattutto quella sterminata galassia di dati che è iCloud, enorme database dei consumi, dei gusti e dei pensieri dei suoi clienti.

Più precisamente, i big di internet condizionano la piena operatività dei loro sistemi (e apparati, nel caso di Apple) alla rinuncia pressoché totale alla privacy da parte nostra: se vuoi usare un iPhone senza lasciare traccia o navigare sul web attraverso Google in modalità anonima devi essere un mostro di bravura, la persona comune non ci riesce, lascia sempre traccia, dice «sì» senza star lì a pensarci quando il sistema chiede consenso, e poi si ritrova sommersa di messaggi pubblicitari magari privi di effetto ma martellanti. Un paradosso che deve finire.

Il Messaggero

Data 27-03-2016
Pagina 15
Foglio 1

L'allarme della Privacy sulle falle del sistema: buchi nella sicurezza

IL DOCUMENTO

ROMA L'anagrafe tributaria, quella che contiene i dati fiscali di tutti gli italiani, compresi quelli dei conti correnti e delle carte di credito, dovrebbe essere, dal punto di vista della sicurezza, a prova di bomba. Le informazioni vitali che sono conservate al suo interno non dovrebbero poter essere viste se non da chi è autorizzato. E si tratta di pochissime persone. La realtà, però, rischia di essere diversa. Il sistema è «vulnerabile». A lanciare l'allarme, qualche settimana fa, era stato il Garante della Privacy, Antonello Soro, che aveva inviato una lettera al ministro dell'Economia, Pier Carlo Padoan, elencando nel dettaglio tutti i "bug", i buchi, riscontrati nel sistema gestito dall'Agenzia delle Entrate. Uno dei principali punti deboli, secondo il garante, è il sistema di controllo degli accessi alla banca dati. Per esempio, spiega Soro, se due utenti accedono con le stesse credenziali, anche da due indirizzi internet diversi, non c'è modo di accorgersene.

Ma il punto più delicato, è proprio quello che riguarda la consultazione dell'archivio dei rapporti finanziari, la porzione della banca dati nella quale sono conservate le informazioni sui conti correnti dei contribuenti italiani. Il protocollo, molto rigido, prevede che per poter accedere ai dati, sia necessaria l'autorizzazione di un soggetto gerarchicamente superiore a chi ne fa richiesta. In pratica servirebbe una doppia chiave per aprire la serratura. Peccato che il software, spiega il garante, identifichi con lo stesso codice fiscale sia chi chiede l'accesso che chi lo deve autorizzare. Di chiave per entrare nell'archivio dei conti correnti, insomma, ne basta anche una sola. Un altro punto debole riguarda gli accessi effettuati dalle forze di polizia e da chi svolge funzioni di giustizia e di sicurezza. Per questi non solo non esistono per niente sistemi di alert che mettano in guardia da accessi anonimi, ma il software non richiede nemmeno di indicare le motivazioni per le quali in questi casi viene effettuata l'interrogazione alla banca dati.

LA POLEMICA

Le anomalie, sempre secondo i risultati dell'indagine del Garante della Privacy, non sono mancate. Dall'analisi degli accessi, per esempio, è emerso che alcuni Comuni hanno effettuato anche 4 mila interrogazioni in un giorno all'anagrafe tributaria, inserendo oltre mille codici fiscali differenti. Un flusso anomalo, ma che non ha generato in automatico, come dovrebbe accadere, il blocco delle utenze.

Dopo l'invio della lettera a Padoan, il direttore dell'Agenzia delle Entrate, Rossella Orlandi, aveva provato a tranquillizzare, sostenendo che molte delle criticità esposte erano già state risolte. Una dichiarazione che aveva fatto alzare il sopracciglio a Soro, che aveva sottolineato come, per il momento, da parte del Fisco fossero arrivate solo delle generiche rassicurazioni che in futuro si sarebbe provveduto a sistemare le cose. Ad oggi, alla vigilia dell'arrivo nell'anagrafe tributaria dei dati sui movimenti dei conti correnti e delle carte di credito del 2015, la questione non sarebbe ancora stata risolta.

Andrea Bassi

LA LETTERA DEL GARANTE ANTONELLO SORO INVIATA AL MINISTRO PADOAN CON L'ELENCO DELLE CRITICITÀ


Conti e carte di credito, via alla super banca-dati

L'allarme della Privacy sulle falle del sistema: buchi nella sicurezza

QN
IL GIORNO il Resto del Carlino LA NAZIONE

Data 30-03-2016
Pagina 1
Foglio 1

Leggi universali per il web

Intervista Il garante Soro: regole nazionali inadeguate, troppo potere ai gestori
Minacce islamiche alla nostra cronista, interviene il sottosegretario Ferri

Silvia Mastrantonio
ROMA

«IL RIFIUTO di Facebook è davvero strano perché, anche in tempi recenti, l'azienda ha dimostrato di voler collaborare, soprattutto in presenza di contenuti di istigazione all'odio. È certo che se il colosso di Cupertino non ha ottemperato a un provvedimento del magistrato questi può procedere con una rogatoria internazionale. Resta, tuttavia, l'anomalia di fondo: la Rete agisce a livello globale, gli ordinamenti restano costretti nei loro ambiti nazionali». Il presidente dell'Autorità Garante per la Privacy, Antonello Soro (**ImagoE**), esamina la vicenda che ha come protagonista la nostra collega, Benedetta Salsi.

«C'è un eccesso di disomogeneità in questo campo. Spesso si deve sottostare alla disponibilità dei singoli gestori mentre, invece, ci sarebbe bisogno di una legislazione armonizzata tra i diversi Paesi per affrontare i fenomeni propri del mondo digitale».

La Rete è considerata il regno della libertà...

«Ma i cittadini, secondo la Risoluzione dell'Onu, hanno il diritto di godere on line degli stessi diritti che hanno off line».

Solo parlare di regole sembra inconciliabile con Internet.

«Per adesso, ci si deve accontentare della disponibilità dei colossi della Rete ma sarebbe nel loro stesso interesse adeguarsi a un insieme di norme armonizzate anticipando quelle che, inevitabilmente, i Paesi dovranno adottare. Così come è avvenuto con il diritto all'oblio che Google ha accettato».

Facebook giustifica il rifiuto a cancellare quelle pagine evitando il discorso del terrorismo e fermandosi alla diffamazione.

«Non è questo che fa la differenza. A volersi nascondere dietro aspetti formali non ci si ricava nulla. Mi spiace che Facebook non abbia colto l'opportunità di dare un'indicazione di tendenza importante. Credo sia stato un errore, soprattutto nell'ambito della sicurezza che rappresenta un argomento sensibile per i cittadini e sul quale l'Europa ha dimostrato, ancora una volta, di non aver abbattuto alcuna barriera».

E nel mondo virtuale?

«Gli imperi del web hanno il dovere di garantire la sicurezza. Tanto più alla luce dei fatti. Penso alla vicenda Apple-Fbi. Apple ha avuto una posizione strumentale che poi è stata superata da Fbi. E si è dimostrato che aprire un singolo telefonino non significa aprire varchi in quelli di tutti gli altri. Che aprire la cassaforte di cui si possiede la chiave, non significa metterle a rischio tutte».

Che cosa conta di più, in questi tempi, la privacy o la sicurezza?

«La privacy è un diritto delle persone, esattamente come lo è la sicurezza. Entrambi questi diritti hanno un rango di tutela altissimo; nessuno, singolarmente, ha più peso degli altri. Anche perché se, per la sicurezza, viene compressa la privacy non è detto che questo porti ai risultati sperati».

A che cosa si riferisce?

«Penso agli esperimenti americani di raccolta dati a tappeto sulle comunicazioni dei cittadini. Una raccolta enorme, la più estesa del mondo che, però, non ha portato i risultati voluti perché è più estesa e più difficile da analizzare».

Come coniugare i due diritti?

«Ci vuole un punto di equilibrio. La privacy va compressa per la sicurezza in modo ragionevole, secondo criteri di proporzionalità. Proprio l'esperienza americana dimostra che contano di più un'indagine selettiva e mirata, la cooperazione tra le diverse forze in campo, la collaborazione che non la raccolta indiscriminata di un volume gigantesco di dati difficile da analizzare».

Facebook ha sbagliato a ignorare l'ordine del magistrato?

«Ha sbagliato e mi auguro che ci ripensi evitando l'attivazione di una rogatoria internazionale. È anche nel suo interesse giungere alla soluzione del problema per conservare la fiducia degli utenti».

CORRIERE DELLA SERA

Data 30-03-2016
Pagina 12
Foglio 1

L'Fbi sblocca il telefono del killer «Non abbiamo bisogno di Apple»

L'aiuto di consulenti esterni. I federali ora analizzano i computer dei terroristi di Bruxelles

DAL NOSTRO CORRISPONDENTE

NEW YORK Trovata la chiave: l'Fbi sblocca l'iPhone di uno dei terroristi di San Bernardino. E con una mossa pragmatica il governo degli Stati Uniti ritira la causa contro Apple, o sarebbe meglio dire contro la Repubblica autonoma di Apple, che si era rifiutata di collaborare.

Tutto ciò accade nello stesso giorno in cui gli investigatori belgi chiedono aiuto ai colleghi americani per decrittare i codici di accesso ai laptop e ai telefonini, recuperati nelle operazioni anti-terrorismo seguite agli attacchi di Bruxelles. Non è una coincidenza. È ormai evidente come un'indagine su larga scala debba impadronirsi dei possibili indizi custoditi nei pc e nei cellulari. Probabilmente lo scontro tra autorità pubblica e industria tecnologica è solo rimandato. L'amministrazione di Washington, in questo caso, ha preferito rinunciare, anche se Melanie Newman, portavoce del Dipartimento della Giustizia, ha chiarito: «Per noi resta una priorità ottenere quelle informazioni digitali che risultano cruciali per garantire la sicurezza pubblica. Lo faremo con la cooperazione delle parti in causa, o attraverso i tribunali se questa cooperazione non dovesse essere possibile». Istruttiva la replica di Apple affidata a un comunicato: «Apple ritiene che il popolo degli Stati Uniti e del mondo intero meriti la protezione dei dati personali, la sicurezza e la privacy. Sacrificare una cosa per l'altra espone le persone e i Paesi a rischi ancora più grandi». Come si vede la società californiana, guidata da Tim Cook, non solo si sente autorizzata a interpretare e a sistemare gerarchicamente i diritti costituzionali. Ma ora parla addirittura a nome «del popolo degli Stati Uniti e del mondo intero», senza spiegare a che titolo, senza dire chi e quando gli abbia mai affidato questo mandato.

L'Fbi non poteva aspettare i tempi della giustizia e gli sviluppi di una causa che, secondo gli esperti, sarebbe potuta arrivare fino alla Corte Suprema. Nell'attentato del 2 dicembre scorso, a San Bernardino in California, furono assassinate 14 persone e ferite 22. I due killer, Syed Rizwan Farook e la moglie Tashfeen Malik, cittadini americani di origine pachistana, si erano ispirati al martirio dei jihadisti. Una cellula isolata? Oppure il nodo di una rete ancora da scoprire? Domande fondamentali e, soprattutto, urgenti.

L'Fbi ha ottenuto la collaborazione di Cellebrite, una società israeliana specializzata in sicurezza digitale. Apple ha già fatto sapere che, a maggior ragione, continuerà il lavoro di ricerca per migliorare l'inviolabilità dei dati.

Giuseppe Sarcina

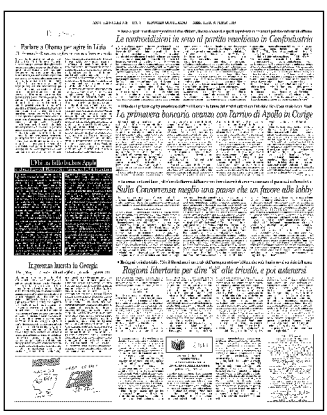
IL FOGLIO

Data 30-03-2016
Pagina 3
Foglio 1

L'Fbi ha fatto ballare Apple

Si chiude il caso dell'iPhone di San Bernardino, il dibattito continua

Questo caso non avrebbe mai dovuto essere portato in tribunale", ha detto Apple in un comunicato dopo che il dipartimento di Giustizia americano ieri ha lasciato cadere l'azione legale contro la società di Cupertino. Chiamata in causa dall'Fbi dopo che si è rifiutata di sbloccare l'iPhone di Syed Rizwan Farook, l'attentatore islamista che a dicembre ha ucciso 14 persone a San Bernardino, Apple ha intrattenuto per mesi un'epica battaglia su privacy, libertà e sicurezza, per essere scaricata dai federali sul più bello. Grazie, abbiamo già fatto, hanno detto. Qualcuno ha sbloccato l'iPhone che credevate inviolabile, non c'è più bisogno di voi. Nelle ultime settimane l'Fbi ha lavorato con un partner esterno per rivelare le informazioni criptate che Apple, adducendo questioni di principio, si rifiutava di estrarre dall'iPhone e che i tecnici del governo americano non erano in grado di ottenere. Secondo report giornalistici, ad aver trovato la chiave sarebbe stata l'israeliana Cellebrite, che giusto la settimana scorsa ha firmato con l'Fbi un contratto da 15 milioni di dollari. Grazie all'ingegno di hacker esterni, dunque, il governo americano è riuscito a rendere superfluo l'intervento di Apple, togliendosi perfino lo sfizio di dimostrare che gli iPhone della compagnia non sono così inespugnabili. Apple dice che la questione, se davvero l'Fbi era in grado di fare da sé, non sarebbe mai dovuta finire in tribunale. Eppure il caso di San Bernardino come nessun altro è riuscito a dare voce alla posizione del governo americano, che poi è la stessa dei governi europei. Serviva un evento polarizzante come un atto terroristico conclamato per spingere l'opinione pubblica a schierarsi, e un avversario di alto profilo come Apple per dare risalto internazionale alla vicenda e scatenare la comunità della sicurezza digitale (che a frotte ha bussato alla porta dell'Fbi per fornire i propri servigi e sbloccare l'iPhone). Il dibattito all'incrocio tra privacy e sicurezza è solo agli inizi, ma l'Fbi, grazie al caso di San Bernardino, è riuscita a definire i termini del discorso pubblico: o con la privacy o con i terroristi. Il dibattito è più complesso di così, e pieno di zone d'ombra ancora da chiarire (per esempio il fatto che sia servita una società esterna per ottenere informazioni che il governo non è stato in grado di estrarre). Ma questa volta l'Fbi ha giocato a scacchi con Apple, e ha azzeccato quasi tutte le mosse.



LA STAMPA

Data 06-04-2016
Pagina 1
Foglio 1

PERCHÉ È GIUSTO SVELARE I SEGRETI

VLADIMIRO ZAGREBELSKY

Quando c'è una fuga o, come ora si dice, «leak» di notizie è perché si tratta di notizie che sono segrete o che c'è chi ha interesse a tenerle segrete. L'ultima fuga, di una serie ormai nutrita, sollecita considerazioni generali che superano la pur importante occasione. E puntualmente l'articolo di Massimo Russo sul giornale di ieri segnala tanti aspetti delle fughe, di cui occorre tener conto per evitare di considerarsene beneficiari, essendo invece strumenti di disegni occulti. Occulti come i «segreti svelati». Occorre certo chiedersi a chi giova la fuga di notizie o, in generale, la pubblicazione di notizie. La risposta alla domanda, se è possibile, serve anche per farsi un'idea della credibilità della notizia. Ma spesso la notizia riflette fatti indiscutibilmente veri, anche se da interpretare. E l'interesse che l'uno o l'altro abbia a svelare il segreto non toglie valore informativo alla notizia sfuggita a chi la deteneva. E ciò tanto più per coloro che non abbiano motivo di parteggiare per chi si avvantaggia della pubblicità data o per chi godeva del segreto.

Tuttavia la domanda a chi giova la pubblicizzazione deve essere accompagnata da quella che chiede a chi giova il mantenimento del segreto. Spesso la risposta è semplice, quando il riferimento è a fatti criminali o altrimenti illeciti o invece a circostanze intime della vita individuale o familiare. Ma vi è tendenza a estendere oltre misura il diritto a mantenere segreti o riservati – come si preferisce dire – ogni genere di fatti e condotte. È il tema della «privacy». L'inglese, come una volta il latino, serve a dare autorevolezza e indiscutibilità a un concetto piuttosto indefinito. E nel discorso pubblico si va molto oltre quanto prevedono le leggi in materia.

La tirannia della trasparenza è denunciata da chi teme che venga travolta l'area di riservatezza indispensabile alla salvaguardia della dignità e della libertà della persona. Ma occorre definire quel nucleo insopprimibile e chiedersi se esso sia eguale per tutti o se vi siano restrizioni per chi esercita funzioni pubbliche o rappresentative, se il limite riguardi anche le condotte che concernono il rapporto con la società e lo Stato, come quelle fiscali, se il limite alla riservatezza riguardi non solo i fatti illeciti, ma anche quelli comunque incompatibili con i doveri propri del ruolo o dello stato professionale. Nella giurisprudenza europea la risposta è affermativa per tutti questi aspetti. I personaggi che sono in qualsiasi modo impegnati nella sfera pubblica sono soggetti a un tasso di pubblicità che la democrazia non richiede per le altre persone. I dati, che riflettono l'osservanza del fondamentale obbligo fiscale, hanno un interesse pubblico che supera quello privato individuale, tanto più quando riguardino persone dalle quali, per la loro ricchezza o posizione, è giusto esigerne il rigoroso adempimento.

Il segreto o riservatezza di informazioni riguardanti le persone è solitamente protetto da norme di legge o dalla imposizione contrattuale di particolari doveri per chi lavora in ambiti privati. È naturale che sia così, poiché spesso chi è interessato al segreto ha anche la forza di imporne le regole. Tuttavia nella società democratica, per consentirne il funzionamento con la formazione di un'opinione pubblica (e un elettorato) consapevole, deve poter operare chi professionalmente o occasionalmente cerca di superare e forzare i segreti. Trovare fonti disposte a correre i rischi derivanti dalla violazione, controllare ed elaborare i documenti e le notizie ottenute, in questo consiste il lavoro del giornalista d'inchiesta. La sua esperienza e correttezza professionale è l'indispensabile condizione perché l'interesse pubblico alla informazione sia adeguatamente soddisfatto e che la pretesa del segreto non sia abusiva.


LA STAMPA

Regeni, l'Egitto offre la prima testa

Renzi: 80 euro in più alle pensioni minime


LA FERMEZZA INCOMINCIA A PAGARE

QUANTO VALE IL PETROLIO D'ITALIA

COSÌ ABBIAMO SCOPERTO IL GREGGIO LUCANO

QN
IL GIORNO Il Resto del Carlino LA NAZIONE

Data 06-04-2016
Pagina 12
Foglio 1 / 2

I giudici non abbassano la guardia «Anche sul web servono regole»

Reggio Emilia, il procuratore Grandinetti: grazie all'ambasciata Usa

Alessandra Codeluppi
REGGIO EMILIA

LE CORTINE di nero sulle due pagine di Facebook sono state calate. Ma, ancora, non è calato il sipario sull'intera vicenda delle minacce rivolte alla cronista del *Carlino* Benedetta Salsi. Facebook, infatti, ha preannunciato un possibile ricorso sulla misura disposta dal giudice del tribunale di Reggio Emilia, Angela Baraldi. E per la procura, che ha seguito le indagini, potrebbero profilarsi nuovi atti per poter dire vinta la battaglia.

Giorgio Grandinetti, procuratore capo di Reggio Emilia, come inquadra sul piano giuridico questa mossa del social network?

«Mi sembra una posizione legittima e in linea con la loro politica di difendere la libertà di espressione. Immagino che Facebook si chieda perché si debbano cancellare tutte le pagine, e non solo i post diffamatori. Non sono sicuro, però, che esista uno strumento per una revoca. Sarà il giudice a valutarne la congruità. Non dimentichiamo che si parla di un ambito scivoloso e complesso. Da parte nostra, aspetteremo eventuali iniziative da parte di Facebook e poi decideremo il da farsi».

Per arrivare alla cancellazione completa disposta dal tribunale, sono occorsi 41 giorni dalla pubblicazione del post e 28 dal decreto del gip, datato 8 marzo. Cosa ha indotto Facebook al dietrofront dopo l'iniziale risposta ('rejected') al giudice?

«Fin dall'inizio abbiamo prestato la massima attenzione al caso, seguito con tenacia dal magistrato Maria Rita Pantani con il supporto della Digos della questura reggiana. E abbiamo fatto capire che non avremmo trascurato alcuna strada, compresa quella di una rogatoria internazionale».

E sul piano dei contatti come si è sbloccato l'intoppo?

«Grazie al dialogo con l'ambasciata Usa, nella persona di Cristina Posa, e con il responsabile Facebook a Londra, che segue l'Italia. Ma credo che anche gli articoli del *Carlino*, dove sono stati rimarcati gli aspetti complessi di questa vicenda, abbiano avuto un peso».

Quali sono state le difficoltà che, come inquirenti, avete incontrato?

«La più grossa è stata far comprendere al rappresentante di Facebook l'istituto giuridico del sequestro preventivo. Per loro non esiste questa misura cautelare. Venerdì, dopo un colloquio con lui durato oltre un'ora, ha ringraziato e assicurato che avrebbe riguardato tutta la vicenda. Ne è seguito poi l'oscuramento avvenuto tra domenica e lunedì».

Questa vicenda, così come lo scontro Apple-governo americano sulla richiesta di dati sul terrorismo, dimostra quanto sia aperto e poco regolamentato il fronte sulla cyber-security. Internet diventa lo spazio di tutti e di nessuno, con rischi per il crimine e la sicurezza.

«Le carenze non sono tanto sul fronte degli accordi bilaterali tra Italia e Usa, che esistono, quanto sull'assenza di convenzioni che si occupino in modo più specifico di questi problemi e delle modalità esecutive dei provvedimenti. Noi inizialmente avevamo scritto alla sezione 'forze dell'ordine' di Facebook, segnalato con un link dedicato. Ma poi il procedimento si è rivelato macchinoso e incerto. Di certo esistono lacune che andrebbero colmate, magari istituendo una figura che possa aiutare a raccordare leggi e provvedimenti di Paesi diversi, e stabilendo norme in un ambito che è ancora poco regolamentato».


RETE PERICOLOSA
I CONFINI DI INTERNET
Facebook oscura la pagina dell'odio
I giudici non abbassano la guardia «Anche sul web servono regole»

La vicenda

L'articolo

Il 25 febbraio sul Carlino di Reggio viene pubblicata in esclusiva una decisione del tribunale su Luca Aleotti, un convertito all'Islam indagato per terrorismo dopo esternazioni sul social in merito alle stragi di Parigi

Minacce e calunnie

L'uomo, destinatario di una «sorveglianza speciale», pubblica sulla pagina 'Musulmani d'Italia', da lui gestita, pubblica un post con minacce, insulti e calunnie alla giornalista autrice dell'articolo

Il braccio di ferro

La procura apre un fascicolo e il giudice dispone l'oscuramento di due pagine sul social network. Facebook rifiuta la richiesta, poi si adegua reputandola però spoporzionata e medita di presentare ricorso

IL CASO Il procuratore capo Giorgio Grandinetti e, a destra, una foto della pagina Facebook 'Musulmani d'Italia'

Il Messaggero

Data 07-04-2016
Pagina 23
Foglio 1 / 2

Svolta per Facebook: tutti i messaggi e le telefonate di Whatsapp saranno automaticamente crittografati. Per la sicurezza, un mercato che vale oro

Criptati e contenti la privacy è un affare

IL CASO

La vostra privacy vale oro. Dopo le rivelazioni di Edward Snowden sulle tecniche di spionaggio della National Security Agency il mondo dell'informatica è cambiato per sempre, tant'è che le major di Internet ora fanno a gara a chi protegge meglio i segreti dei propri utenti. Anche l'attenzione che ha suscitato a livello mondiale il braccio di ferro tra la Apple e l'Fbi per lo sblocco del telefonino del terrorista di San Bernardino, la dice lunga al riguardo. Non sorprende quindi che anche le cosiddette "chat-app" si stiano adeguando alla nuova moda. Chi utilizza Whatsapp lo sa bene. Gli utenti della app di messaggistica di Facebook si sono visti recapitare in queste ore un avviso che non è passato inosservato: «I messaggi che invii in questa chat e le chiamate sono ora protetti con la crittografia end-to-end».

IL PROBLEMA

Whatsapp lavorava al progetto dalla fine del 2014. Ora tutti i messaggi e le chiamate vocali che passano sulla piattaforma vengono automaticamente criptati. Ma in cosa consiste la cifratura end-to-end? In pratica si basa sull'uso di un sistema crittografico che rende illeggibile la comunicazione tra due dispositivi. La mossa della app di messaggistica arriva in un periodo di forti tensioni e di dibattiti sul tema della criptazione e della sicurezza dei dati online. Non si tratta però solo di business. È anche una questione di potere. Si potrebbe persino dire di sovranità nazionale.

I big di Internet, da Whatsapp a Facebook, da Twitter a Google, rassomigliano sempre di più a dei veri e propri Stati, con un Pil degno di un Paese di sviluppo e milioni di abitanti 2.0. Per loro difendere i dati degli utenti equivale per certi versi a difendere i confini virtuali che li delimitano.

«Riconosciamo il lavoro importante delle forze dell'ordine nel tenere le persone al sicuro ma gli sforzi per indebolire la cifratura dei dati espongono le informazioni delle persone all'abuso di cybercriminali, hacker e stati canaglia», ha scritto la compagnia sul suo blog al momento di annunciare la novità.

I CONCORRENTI

Whatsapp (un miliardo di utenti) è corsa ai ripari a fronte anche del crescente successo del concorrente Telegram. Telegram è un'app di messaggistica sviluppata in Russia, con circa 100 milioni di utenti all'attivo, che cripta i messaggi con algoritmi molto potenti. Anche su Signal però i messaggi sono tutti criptati end-to-end. Line offre invece l'opzione "lettera sigillata" che rende impossibile la lettura del messaggio da parte di un soggetto terzo. L'app di messaggistica Cyber Dust addirittura distrugge i messaggi una volta che sono stati letti dal ricevente.

La corsa alla privacy non risparmierà nemmeno i server. Whatsapp, per esempio, ha detto a più riprese di non archiviare i messaggi sui propri server. I messaggi inviati da un dispositivo Apple a un altro rimangono criptati anche sui server. Al contrario, le comunicazioni che passano per Google Hangouts restano criptate sui server ma Google è in grado di decifrarle e quindi potrebbe fornirne i dettagli alle autorità che ne dovessero fare richiesta. Nel caso di Skype i messaggi vengono conservati allo stato naturale sui server per un periodo limitato. Anche l'app per le chiamate VoIP Viber conserva sui server le comunicazioni in un formato non criptato. La cinese QQ, app di messaggistica del colosso Tencent, cripta i messaggi solo durante il transito fra il telefono dell'utente e i server dell'azienda: in caso di necessità i messaggi quindi possono essere letti sia da QQ che dalle forze dell'ordine.

IL MARKETING

Nel film "Perfetti sconosciuti" di Fabio Genovese lo smatphone viene paragonato a una scatola nera contenente tutti i segreti di una persona. E in parte è così. Ma le parole di Jan Koum, fondatore della piattaforma di Whatsapp, che ha annunciato sul suo profilo Facebook la svolta della compagnia, lasciano intendere che si tratta anche di una questione di principio. «Sono cresciuto in Russia durante il regime comunista, quando la gente non poteva parlare liberamente, pure per questo il desiderio di proteggere la comunicazione privata delle persone è uno dei principi base di Whatsapp», ha scritto Koum.

Ma dietro c'è dell'altro. La crittografia introdotta da Whastapp è anche una mossa di marketing. In un'era in cui la privacy ha assunto un peso determinate nell' ambito della sicurezza informatica, al fine di conquistare nuovi

segmenti di mercato le aziende del settore non possono non proteggere le comunicazioni delle persone. Anche Facebook intende incrementare la sicurezza del suo Messenger. Pure Snapchat sta lavorando a un sistema più sicuro. Mentre Google è impegnato nel portare a termine il progetto sulle email criptate "End to end" avviato nel 2014.

Francesco Bisozzi

IL MATTINO

Data 07-04-2016
Pagina 1
Foglio 1

I messaggi cancellati non potranno più essere letti da nessuno

Privacy, non ci resta che WhatsApp

Francesco Durante

Segue dalla prima

Privacy, non ci resta che WhatsApp

Avendo lavorato per una vita nei giornali, serbo memoria di certi capiredattori del tempo che precede l'invenzione del cellulare, i quali avevano il vezzo di terminare qualsiasi conversazione telefonica più o meno riservata con la seguente formula: «Buonasera anche a lei, maresciallo». Voleva alludere (un po' gigionescamente, non c'è che dire) al fatto che poteva esserci qualcuno che quella telefonata l'aveva discretamente intercettata e ascoltata. Da quell'epoca – un'epoca in cui non c'era nemmeno il fax – ogni cosa è cambiata.

Francesco Durante

Soprattutto, sono arrivati i telefonini, e miliardi di persone hanno imparato prima a scambiarsi chiamate e messaggini, poi hanno scoperto le nuove app, e soprattutto l'attuale regina della comunicazione istantanea, non a caso acquistata per 19 miliardi di dollari da mr Facebook Mark Zuckerberg, vale a dire WhatsApp.

E insomma ora, mentre ancora non si sono del tutto placate le polemiche intorno al rifiuto di Apple di fornire alla Fbi le chiavi d'accesso all'iPhone del terrorista di San Bernardino, WhatsApp annuncia l'adozione della crittografia «end-to-end», che sarebbe quella tecnica grazie alla quale messaggi e chiamate sono visibili soltanto ai due soggetti che stanno comunicando fra loro, e lo fa per l'appunto nascondendo messaggi e chiamate a tutti gli altri, compresa la società che fornisce il servizio. Bisognerà poi vedere se la Fbi, che alla fine è riuscita da sola a violare il sistema di sicurezza dell'iPhone le cui chiavi le erano state negate dal grande capo Tim Cook, saprà avere ragione anche di questo nuovo muro.

Nella società dell'ipersorveglianza (copyright Jacques Attali), una notizia come questa è insieme buona e cattiva. Buona perché mette a disposizione di centinaia di milioni di persone uno strumento che ne può difendere seriamente la privacy molto meglio di quanto non sappiano fare i telefonini di fascia più popolare. Altro che «buonasera maresciallo»: d'ora in poi ci si potrà affidare a WhatsApp per tutte quelle cosette quotidiane su cui intendiamo mantenere un rigoroso riserbo. Dunque, per fare un esempio, niente più coniugi fedifraghi beccati a mandare un messaggino all'amante (e, meglio ancora, niente più pm pronti a captarlo con la rete a strascico di un'intercettazione finalizzata a scoprire altre faccende). Possiamo dire che, benché centinaia di occhi ci seguano passo passo nelle nostre città e altrettanti orecchi ci ascoltino, almeno ci resta questa bolla di (relativa) tranquillità. La cattiva notizia è che ovviamente potremmo decidere di farne cattivo uso: nel qual caso, all'aumento della nostra sicurezza corrisponderebbe la diminuzione di quella altrui.

Dicono peraltro quelli che hanno dimestichezza con queste cose che ciò che WhatsApp annuncia adesso, tanti altri già da tempo le offrono ai loro clienti. E aggiungono che, nella maggior parte dei casi, quello della totale inviolabilità dell'applicazione è più un mito che una realtà effettiva, giacché tutto poi dipende dalla capacità delle persone di servirsi al meglio degli strumenti messi a loro disposizione. Bisogna insomma essere capaci di attivare il livello di protezione desiderato, e la cosa non è proprio da tutti. In ogni caso, resta il fatto che la scelta di WhatsApp, proprio in quanto rivolta a una platea enorme di utenti, rappresenta un passo abbastanza memorabile. Di sicuro, prima o poi qualcuno saprà trovare il modo di «craccare» la app malgrado i suoi nuovi superpoteri. Nell'attesa di questo prevedibile esito, fate dunque un'esilarante indigestione di libertà. Dietro le quinte, almeno per un po', non ci sarà nessuno pronto, per dirla con Foucault, a sorvegliare e punire.

maildurante@gmail.com

l'Unità

Data 09-04-2016
Pagina 13
Foglio 1

La reazione ai cyber attacchi

Michele Pierri
DIRETTORE
DI "CYBER AFFAIRS"

Crescono cyber crime, spionaggio industriale e terrorismo cibernetici. E, con essi, il bisogno dei cittadini a sentirsi più protetti, e delle istituzioni e delle imprese ad adottare strumenti di governance e sicurezza sempre più avanzati.

Mentre una delegazione del Laboratorio nazionale di cyber security del Consorzio Cini è in queste ore a Washington per rafforzare gli scambi e la cooperazione cyber con l'altra sponda dell'Atlantico, molto resta ancora da fare sul piano domestico. E quanto ampio sia il perimetro delle azioni da intraprendere e la varietà dei soggetti da coinvolgere per creare un sistema Paese davvero resiliente alle minacce cyber è riemerso martedì, quando esperti ed addetti ai lavori italiani e internazionali si sono confrontati per discuterne a Roma durante il Cybersecurity summit di "The Innovation Group".

Non sono solo le infrastrutture critiche a dover essere poste sotto osservazione.

La portata dell'odierna sfida cibernetica, ha evidenziato il direttore della Polizia Postale e delle Comunicazioni Roberto Di Legami, deriva innanzitutto dal cambiamento sempre più veloce dei nostri stili di vita quotidiani. Gli oggetti "smart", perennemente connessi alla Rete, sono innovazioni che generano «un'opportunità», ha detto Di Legami, ma rappresentano al tempo stesso un «moltiplicatore di vulnerabilità» e «un pericolo» da cui imparare a difendersi. C'è poi, ha aggiunto, una questione specifica di sicurezza legata all'uso intensivo degli smartphone privati, meno protetti delle reti aziendali, ma attraverso i quali si usufruisce ormai di moltissimi servizi e spesso e volentieri si accede anche a informazioni di carattere lavorativo (con tutti i rischi che ne conseguono). A ciò si somma un tema più ampio, riguardante la sensibilità degli utenti. «Il fattore umano è importantissimo», ha spiegato Di Legami. Molti attacchi vanno in porto per la poca attenzione o la scarsa conoscenza informatica da parte delle persone colpite.

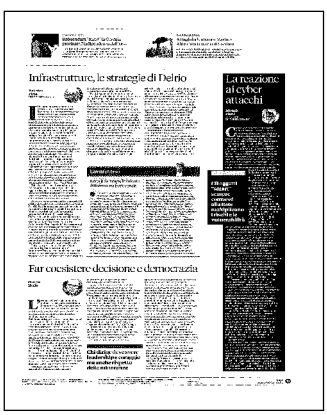
Ma il tema di un cambiamento culturale sul fronte della cyber security non coinvolge solo gli elettori, ma anche i loro eletti.

«I governi, compreso quello italiano - ha sottolineato il consulente Andrea Rigoni a Cyber Affairs - , devono cominciare ad affrontare i problemi di cyber sicurezza con un approccio strategico», ovvero, «costituendo una guida per la Difesa, il law enforcement e il settore privato», chiamati poi a mettere in sicurezza col sostegno di altri attori l'intero ecosistema. «Serve in fretta una strategia nazionale estensiva», ha rimarcato, perché le minacce non aspettano, anzi si intensificano, come suggeriscono i dati più recenti.

Sul fronte del cyber crime, ha raccontato Rita Forsi, direttore dell'Iscom, l'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione del ministero dello Sviluppo economico, si assiste a «un significativo aumento» degli episodi di "phishing", ovvero le truffe su internet che sfruttano tecniche di ingegneria sociale per ingannare le vittime portandole a fornire a malintenzionati le loro informazioni personali, dati finanziari o codici di accesso.

Reagire si può.

L'obiettivo a cui si lavora, ha detto ancora la Forsi, è che il Cert nazionale - una struttura che, sulla base di un modello cooperativo pubblico-privato, supporta cittadini e imprese attraverso azioni di sensibilizzazione, di prevenzione e di coordinamento della risposta ad eventi cibernetici - arrivi «ad analizzare sempre più dati forniti» dalle segnalazioni, «per poi mettere i risultati a disposizione sia di chi è vittima degli attacchi sia di chi utilizza questi dati per scopi convergenti, come le Forze di Polizia».


Infrastrutture, le strategie di Delrio

La reazione ai cyber attacchi

Far coesistere decisione e democrazia

Il Sole 24 ORE

Data 10-04-2016
Pagina 20
Foglio 1

Caso Apple. La privacy e l'identità digitale pubblica

Le tracce dei dati e le libertà in pericolo

di **Franco Debenedetti**

Si vedono sempre più porte con una serratura nuova: è quella che neutralizza la cosiddetta chiave bulgara, inesorabile contro le serrature tradizionali. Un'innovazione tecnologica ci aiuta a difendere i beni che custodiamo nelle nostre case, e i valori, economici, simbolici, affettivi, che ne fanno la nostra "proprietà".

Chiavi, serrature, proprietà sono al centro della battaglia ingaggiata dall'Fbi contro Apple. I "federali" esigevano che la società di Cupertino fornisse la chiave per aprire lo smartphone di uno degli autori della strage di San Bernardino, ma l'azienda si rifiutava: non voleva venir meno alla assicurazione fornita ai suoi clienti, di aver munito l'ultima versione dell'iPhone con una "serratura" in grado ci proteggere la loro "proprietà". La posizione dell'Fbi non sembrava fortissima: perché è difficile sostenere che eliminare la serratura sia un modo efficace di contrastare i ladri, compresi quelli elettronici; perché non sembra essere nei poteri di un'agenzia di investigazione imporre a un'azienda che prodotto deve fare; infine, ed è l'argomento decisivo, perché stabilire se ed in quali limiti sia consentito crittografare, deve farlo il parlamento con una legge, non un tribunale con una sentenza. Non sono la guardia finanza o l'agenzia delle entrate che hanno abolito il segreto bancario, ma accordi tra Stati. In ogni modo ci ha pensato una società israeliana a cavare d'impaccio l'Fbi, annunciando di avere trovato la "chiave" per forzare la "serratura".

Trovare l'analogo elettronico di "chiavi" e "serrature" è intuitivo: più complicato individuare l'analogo di "proprietà". Lo sono ovviamente i testi che scriviamo, i calcoli che facciamo, i dati che organizziamo, le comunicazioni scritte e orali: sono nostra "proprietà", alla stessa stregua dei beni di casa. Ma c'è anche l'immensa quantità di altri dati che la tecnologia digitale consente di acquisire, e che Big Data sa come conservare, ordinare, confrontare: sono le tracce che noi lasciamo dietro di noi. Nell'era digitale, le tracce sono la circunstancia del famoso detto di Ortega y Gasset. «*Yo soy yo y mi circunstancia, y si no la salvo a ella no me salvo yo*». Tracce sono la nostra posizione rilevata dalle app, i nostri libri acquistati da Amazon, i nostri viaggi prenotati da Booking. Noi accettiamo che esse vengano "salvate" perché questo ci serve per "salvare" noi stessi, la nostra identità: perché da un lato ne ricaviamo vantaggi di cui non sapremmo più fare a meno, e dall'altro ci sentiamo garantiti da un contratto, esplicito o implicito, che quei dati non saranno mai usati nominativamente.

Lasciamo tracce anche quando spendiamo i nostri soldi: anzi, questa è forse la *circunstancia* più legata alla nostra identità, che quindi gelosamente custodiamo. Libertà è (anche) libertà di disporre dei propri averi, senza doverne rendere conto ad altri contro la nostra volontà. La legge (il Salva Italia di Monti) vuole rendere tracciabili le tracce: da aprile gli operatori finanziari dovranno automaticamente trasmettere all'Agenzia delle Entrate movimentazioni dei conti correnti, saldi, giacenze, investimenti, carte di credito, bancomat, accessi alle cassette di sicurezza. La legge originariamente faceva riferimento a "liste selettive " di contribuenti sospetti, adesso ad una più generica "analisi del rischio di evasione": basta per condividere l'ottimismo di Antonello Soro, garante della privacy, per cui questa nuova formulazione «impedisce di fatto un controllo generalizzato e diffuso di tutti i contribuenti»? Impedisce? Di fatto? Miliardi di dati solo per «l'analisi del rischio»? A preoccupare non è la fase di contestazione di evasione e il successivo accertamento, dove ci sono procedure e garanzie, ma quella di "analisi del rischio", che potrebbe finire come intrusione in dati personali. Vederci il grande fratello è probabilmente paranoia; ma non è esagerato temere che i nostri dati vengano usati per profilarci, o finiscano nelle mani di un funzionario infedele, o vengano intercettati da un hacker. Almeno si limiti il tempo oltre il quale i dati devono essere distrutti: sei anni ha chiesto il garante, e sembrano davvero troppi. Per farsi aprire la porta di casa, le forze dell'ordine devono avere un decreto del magistrato: qui tutte le porte sono state aperte, e nessuno garantisce l'uso corretto di ciò che si trova. Che almeno ci sia un'autorità terza, con i poteri e mezzi tecnici per certificare metodologie e procedure, e per verificare che vengano applicate.

Cambia la tecnologia: ma è sempre una questione di "chiavi" e di "serrature": e di "proprietà".


Le elezioni Usa e la caduta dei valori

Le tracce dei dati e le libertà in pericolo

CORRIERE ECONOMIA

Data 11-04-2016
Pagina 18
Foglio 1

edoardosegantini2@gmail.com

L'analisi

La privacy non è un impiccio ma servono dati «di qualità»

DI **EDOARDO SEGANTINI**

Nel suo libro edito da Codice Edizioni («Liberi e connessi»), il Garante della Privacy Antonello Soro affronta gran parte dei temi legati al suo incarico (dal diritto all'oblio alla trasparenza, dalle intercettazioni al processo mediatico, dalla reputazione online al controllo a distanza). Ma in realtà i punti che sembrano stargli veramente a cuore sono due.

Il primo: «La protezione dei dati non è un limite per l'economia, ma al contrario è uno dei principali fattori di crescita e innovazione». Non è un'affermazione scontata. Crisi economica e terrorismo hanno convinto molti (anche tra i decisori pubblici) che la difesa della privacy sia un impiccio che frena le aziende e indebolisce gli interventi contro i terroristi. Per Soro è vero il contrario.

Le imprese e le amministrazioni che difendono il patrimonio informativo, scrive il Garante, in realtà difendono se stesse. La sicurezza può diventare un valore aggiunto. Per contrastare il terrorismo, scrive, «abbiamo più bisogno di selezione che di quantità».

Ciò che è mancato dopo la strage del Bataclan a Parigi (come in altri casi) non è il numero delle informazioni, ma una loro analisi efficace. Più che «schedature di massa» attraverso «leggi speciali», dice Soro come i migliori magistrati italiani, serve un'azione investigativa mirata e transnazionale. Secondo punto: i dati si valutano, non si pesano. Cattiva qualità genera trasparenza sbagliata. Se c'è un modo efficace di nascondere un'informazione importante è quello di annegarla in un mare di dati inutili. Come fanno gli avvocati nei romanzi di Grisham, quando sommergono gli avversari di scatoloni di carte.

«Un eccesso informativo (e normativo) — scrive Soro forse anche a proposito del Freedom of Information Act approvato dal governo nel gennaio scorso, di cui auspica una revisione — aumenta il grado di opacità dell'ordinamento e, conseguentemente, di inosservanza e inefficacia delle norme».

Ad esempio: è proprio necessario, per controllare l'azione amministrativa, pubblicare in rete lo stato patrimoniale di tutti i componenti (e dei relativi congiunti) del senato accademico, ivi inclusi gli studenti, anche per le università non statali? Serve davvero conoscere i compensi di ogni dirigente scolastico del Paese? Evidentemente no, a meno che non si preferisca la demagogia a una trasparenza realmente democratica.

Emerge, in finale, una clamorosa asimmetria fra il mondo pubblico, che i dati dei cittadini non sa gestire, e il vantaggio commerciale che al contrario ne traggono i giganti della Rete. Senza che i legittimi proprietari dei dati medesimi (ognuno di noi) chieda il diritto di negoziarne l'uso. Insomma: connessi lo siamo (anche se male), liberi proprio no. Qualcuno la chiamerebbe «libertà vigilata».

@SegantiniE

l'Unità

Data 15-04-2016
Pagina 11
Foglio 1

«Cyber-security, solo lo scambio informativo può renderla efficace»

● Il colonnello Paolo Puri, consigliere militare di Palazzo Chigi: è necessaria una regia unica

● «Va allargata la diffusione della cultura cibernetica, e non solo tra gli addetti ai lavori»

Michele Pierri

L'inarrestabile digitalizzazione di istituzioni e imprese e la moltiplicazione degli oggetti connessi alla Rete – l'Internet delle Cose - stanno cambiando l'approccio alla cyber security. La protezione dello spazio informatico non è più solo materia per esperti, ma sta rapidamente evolvendo in un fattore cruciale per la competitività economica di un Paese, capace di decidere la sua capacità di proteggere know how e dati personali, e di conseguenza di attrarre investimenti. E coinvolge ormai la vita quotidiana di ogni cittadino: dalle auto ai frigoriferi non c'è oggetto che nei prossimi anni, e in parte già adesso, non sia destinato a essere vulnerabile per l'attacco di un hacker.

Non stupisce, pertanto, l'attenzione e la rilevanza che il tema assume giorno dopo giorno anche nel nostro Paese, tanto sui media quanto nelle valutazioni dei decisori ai più alti livelli.

«Spesso», ha rilevato il colonnello Paolo Puri, consigliere militare vicario del presidente del Consiglio, «si sente parlare di una eventuale rivisitazione dell'architettura istituzionale cyber» italiana. «Se questo avverrà», ha sottolineato, «comunque sarà fondamentale l'individuazione di attori con compiti, ambiti applicativi e mandato chiari e ben definiti».

In un'eventuale azione di riordino della cyber security italiana, ha spiegato l'alto ufficiale in un'intervista a Cyber Affairs a margine di un evento organizzato a Roma dall'Associazione italiana esperti infrastrutture critiche, «è necessario che il legislatore armonizzi in un unico corpo normativo l'intero settore della difesa cibernetica permettendo, in tal modo, che la complessità della materia trovi riscontro in una esaustiva e lineare gestione, requisito essenziale per una strategia efficace».

Se, ha commentato Puri, «da un lato potrebbe esservi l'esigenza di posizionare il Nucleo per la sicurezza cibernetica» (a cui è affidato il raccordo tra tutte le amministrazioni) «in un ambito probabilmente più idoneo rispetto all'attuale collocazione» (attualmente è presieduto dal consigliere militare del presidente del Consiglio dei ministri), «dall'altro si avverte la necessità di rafforzare l'autorevolezza del Cert Nazionale», una struttura che, sulla base di un modello cooperativo pubblico-privato, supporta cittadini e imprese attraverso azioni di sensibilizzazione, di prevenzione e di coordinamento della risposta ad eventi cibernetici.

Questo organo «che deve agire da raccordo tra le esigenze di sicurezza delle organizzazioni private e quelle pubbliche», ha rilevato ancora, «assolve al delicatissimo ruolo di garante l'infosharing tra i vari Cert, italiani ed internazionali, e le aziende. Lo scambio informativo, effettuato in maniera sicura e tempestiva, è alla base della cyber defense e dell'information assurance ed è un presupposto imprescindibile per la gestione degli eventi ai vari livelli e, ove necessario, per l'escalation di eventuali crisi nello spazio cibernetico».

Per quanto concerne la condivisione degli obiettivi tra i vari attori interessati, invece, ha rimarcato Puri, «credo che questo rappresenti un tasto dolente del modo con cui le materie delle infrastrutture critiche, della sicurezza cibernetica ed, in ultima analisi, del settore della gestione delle crisi sono state affrontate in Italia negli ultimi anni».

L'approccio, ha sottolineato, «è stato, in molti casi, poco efficace perché i settori sono stati normati senza aver cercato di eliminare le endemiche divisioni tra le amministrazioni o tra i settori che storicamente si sono occupati di queste materie. Ciò ha fatto si che gli sforzi, seppur apprezzabili, siano stati scoordinati, senza una regia unica che si occupasse anche di verificare il raggiungimento degli obiettivi e, pertanto, i risultati sono stati parziali».

Un'efficace sicurezza delle informazioni, ha detto ancora il consigliere militare vicario di Palazzo Chigi, «non potrà esservi se non vi saranno degli sforzi costanti nel campo della formazione dei cittadini, studenti, imprese e dipendenti della Pubblica amministrazione. La promozione e la diffusione della cultura cibernetica», ha concluso, «deve essere allargata a tutte le categorie menzionate e non essere soltanto materia per gli addetti ai lavori».

Finora l'approccio in molti casi ha portato solo risultati parziali

La protezione dello spazio informatico cruciale per la competitività economica del Paese

CORRIERE DELLA SERA

Data 15-04-2016
Pagina 1
Foglio 1

Microsoft fa causa al governo americano

Il gigante informatico reclama il diritto di comunicare ai clienti quando le loro mail sono intercettate

WASHINGTON E' lotta continua. Da una parte il diritto alla privacy, dall'altro le esigenze di sicurezza. Le grandi compagnie di comunicazione contro l'ingerenza di chi indaga.

L'ultima battaglia l'ha ingaggiata in tribunale la Microsoft. La società americana ha citato in giudizio il Dipartimento della Giustizia, una mossa dura per rispondere a pressioni non meno forti. In base alle norme, la ditta non può rivelare ai suoi clienti che le autorità federali hanno accesso a dati e email. Dunque una violazione - sostengono i legali - a quanto sancito dalla Costituzione statunitense. Gli avvocati si trincerano dietro due posizioni: il primo e quarto emendamento che garantiscono libertà di espressione e il diritto di essere avvertiti se lo Stato fruga nel privato. Elementi che fanno ben comprendere il livello dello scontro, diventato sempre più aspro dopo il ripetersi di attacchi terroristici.

Gruppi criminali ed affiliati a movimenti eversivi — come l'Isis — sono spesso al centro di indagini in cui i loro contatti digitali, dalla posta elettronica al traffico telefonico, rappresentano un aspetto chiave. Gli inquirenti cercano di usare le informazioni recuperate per ricostruire rapporti, relazioni, persino viaggi. E dunque gettano la rete chiedendo collaborazione piena e incondizionata da parte di chi fornisce i servizi al pubblico.

In passato ci sono state anche consultazioni con l'amministrazione per trovare un terreno comune, ma il dialogo ha portato a poco. Il braccio di ferro si è riproposto, infatti, con Twitter e Google. Diatriba finita al Congresso, che ha provato a mediare ipotizzando un meccanismo che prevede un ritardo di sei mesi nella notifica ai clienti dell'avvenuto intervento federale.

Sempre i parlamentari sono stati chiamati in causa per un altro duello, quello che ha opposto la Apple all'Fbi dopo la strage di San Bernardino. Si chiedeva un loro intervento sul rifiuto del gruppo di rendere accessibili gli iPhone dei terroristi agli investigatori. Solo che gli agenti hanno scelto una scorciatoia e sono entrati nei cellulari usando non la «porta» ma la «finestra». Con una procedura che ha sollevato polemiche il Bureau si è affidato agli hacker ingaggiati «a tariffa fissa» con il compito di scardinare il sistema del telefonino. Inizialmente si era pensato che la polizia federale avesse avuto l'aiuto di maghi dell'hi-tech israeliani, tecnici in grado di perforare la corazza dell'apparato. Una versione di comodo superata da indiscrezioni emerse in questi giorni che hanno confermato come fossero stati altri i protagonisti dell'incursione. Ma l'operazione ha dato dei risultati? Forse è presto per una risposta definitiva. Secondo una fonte citata dai media dopo un primo esame dell'iPhone non sarebbero emersi aspetti interessanti su Syed Farouk e su possibili complici.

Fino ad oggi la tesi ufficiale è che il killer abbia agito insieme alla moglie in modo autonomo, probabilmente ispirato solo a livello ideologico dalla propaganda del Califfo. Una coppia di assassini che ha portato in dote il massacro allo Stato Islamico, senza avere dei legami operativi stretti. Diverso il comportamento del commando responsabile degli attacchi in Francia-Belgio: ha usato sistemi criptati o telefonini usa e getta.

Guido Olimpio
@guidoolimpio

Braccio di ferro
I legali della società sostengono che si tratta di violazione della Costituzione


CORRIERE DELLA SERA
Referendum, attacco di Renzi


Microsoft fa causa al governo americano
UNOPIU'

Il Sole 24 ORE

Data 15-04-2016
Pagina 7
Foglio 1

La lotta al terrorismo
LA RISPOSTA EUROPEA

Come funzionerà
Ciascun governo costituirà un archivio con i dati dei viaggiatori in partenza e arrivo da Paesi terzi

I punti deboli
I Paesi non sono obbligati a condividere i dati trasmessi dalle compagnie

Aerei, schedati i passeggeri in Europa

Dopo 5 anni l'Europarlamento approva la direttiva sul Pnr in funzione anti-jihad

Beda Romano
BRUXELLES. Dal nostro corrispondente

Dopo cinque anni di tira-e-molla negoziale, il Parlamento europeo ha approvato ieri a Strasburgo una attesa direttiva con la quale verrà creato l'abbozzo di una banca dati europea per i passeggeri aerei. La partita non è stata semplice, segnata dalla lotta anti-terrorismo, ma anche dalle gelosie nazionali di alcuni e dai timori per la privacy di altri. Nel contempo, sempre ieri l'assemblea ha dato il suo benestare a un'altra direttiva, volta a tutelare il segreto commerciale delle imprese.

La nuova direttiva, nota con l'acronimo inglese PNR (Passenger Name Record), prevede che ciascun paese adotti un proprio schedario in cui raccoglierà le informazioni dei passeggeri sui voli in partenza o in arrivo da paesi terzi. Parlare di vera e propria banca dati europea è quindi improprio. «Grazie alla raccolta, alla condivisione e all'analisi dei dati le agenzie di intelligence potranno notare eventuali comportamenti sospetti», ha spiegato il relatore del testo, l'eurodeputato Timothy Kirkhope.

Il tentativo è di lottare contro il rischio terroristico. L'uomo politico conservatore inglese ha però ammesso che la direttiva «non è un rimedio miracolo». Infatti, le compagnie aeree avranno l'obbligo di trasmettere i dati alle singole autorità nazionali, ma i paesi non saranno obbligati a condividerli tra loro. L'obbligo della raccolta, poi, riguarda i voli con i paesi terzi. Per quanto riguarda i voli nazionali o i voli intra-europei varrà la volontarietà.

I governi avevano trovato un difficile compromesso alla fine del 2015, su pressione in particolare della Francia dopo gli attentati del 13 novembre scorso. La partita è stata segnata da un doppio obiettivo non facile da conciliare: rafforzare la collaborazione europea nella lotta anti-terrorismo e garantire comunque la privacy dei cittadini. Non per altro il voto di ieri a Strasburgo è stato incerto fino all'ultimo. I liberali hanno chiesto, senza successo, che lo scambio dati fosse automatico.

Sempre ieri, il Parlamento europeo ha anche approvato una altra direttiva, questa volta dedicata alla protezione delle aziende nel caso di furti di segreti commerciali. Secondo le statistiche comunitarie, ogni anno una società su cinque è vittima di furto. Prima di tutto, il testo adotta una definizione comune di segreto commerciale. In secondo luogo, il provvedimento dovrebbe facilitare il risarcimento dell'impresa che subisce l'estorsione, con alcuni limiti, tuttavia.

Infatti, al momento del negoziato con i Ventotto, il Parlamento europeo ha insistito perché fosse introdotta una clausola, a dire il vero piuttosto generica, per garantire comunque «la libertà di stampa, il pluralismo dei media e il lavoro dei giornalisti, facendo riferimento in particolare alle loro inchieste e alla tutela delle fonti». Sulla scia della pubblicazione delle Panama Papers, la questione di come proteggere gli informatori della stampa ha influenzato il dibattito della vigilia.

Infine, l'assemblea parlamentare, riunita questa settimana in sessione plenaria a Strasburgo, ha adottato anche un pacchetto che aggiorna dopo 20 anni le regole europee sull'uso dei dati personali all'epoca di internet. Un primo regolamento definisce i diritti dei cittadini sull'uso da parti di terzi delle proprie informazioni personali, garantendo tra le altre cose il diritto all'oblio. Una seconda direttiva, invece, stabilisce come questi stessi dati possano essere utilizzati dalle autorità di polizia e giudiziarie.

Domande & risposte

Nel database dal nome alla carta di credito

Cosa è il Pnr?
Il Passenger name record (acronimo Pnr) è l'insieme delle informazioni fornite dai passeggeri e raccolte dalle compagnie aeree al momento della prenotazione/acquisto dei biglietti e del check-in. Vi potranni rientrare anche quelle raccolte da agenzie di viaggio e tour operator che usino voli charter ma soltanto se i singoli Stati lo decideranno su base volontaria.

Quali dati rientrano nel Pnr?
Sono numerose le informazioni che finiscono nel data record: date e itinerario del viaggio, partenza, destinazione, modalità di pagamento, numeri di contatto, notizie sui bagagli.

Quando scatterà la raccolta dei dati?
I dati dovranno essere obbligatoriamente raccolti soltanto quando il volo sia tra un paese terzo (esterno all'Unione europea) e parta da o arrivi in uno Stato membro. Un registro dei dati relativi ai voli intra-Ue potrà essere creato ma soltanto su base volontaria. Si tratta di un limite importante dell'efficacia del nuovo strumento perché i recenti fatti di cronaca e le analisi degli esperti hanno dimostrato che i movimenti dei terroristi avvengono soprattutto all'interno dei paesi Ue essendo i terroristi cittadini di Stati Ue diventati "foreign fighters".

Chi avrà accesso ai dati?
Le compagnie aeree manderanno le informazioni alle "autorità competenti" dello Stato membro interessato che non avrà accesso diretto ai database delle stesse.
I dati verranno inviati a un centro appositamente creato, la Unità di informazione sui passeggeri (Uip, Piu in inglese) dello Stato interessato. Ogni Stato membro dovrà redigere una lista delle autorità competenti alle quali la Uip darà i dati grezzi ricevuti oppure il risultato della loro elaborazione. Quest'ultima, insieme alla conservazione dei dati, dovrà essere effettuata da ciascuna Uip nazionale.

Gli Stati potranno condividere le informazioni?
Le autorità nazionali dovranno allertare gli altri Stati membri e condividere le informazioni delle loro analisi al fine di prevenire o perseguire reati gravi quali terrorismo internazionale, traffico di essere umani, traffico di droga, pedopornografia. Gli Stati membri, inoltre, potranno chiedere dati del Pnr per specifiche inchieste.

Per quanto tempo verranno conservati i dati?
Le informazioni verranno conservate per cinque anni ma dopo sei mesi verranno rese anonime mediante la mascheratura di alcuni elementi come il nome e i contatti.

Sono stati stabiliti divieti nella raccolta di informazioni?
Sì. La direttiva stabilisce che gli Stati membri dovranno vietare un trattamento che riveli l'orgine razziale o etnica, le opinioni politiche, la religione, l'appartenenza a sindacati, lo stato di salute o l'orientamento sessuale dei passeggeri.

A CURA DI
Roberta Miraglia

ItaliaOggi

Data 15-04-2016
Pagina 30
Foglio 1

Via libera al pacchetto dall'Europarlamento. Ci saranno due anni per organizzarsi

Regole privacy in stile europeo

Diritto all'oblio e data protection officer in imprese e p.a.

DI ANTONIO CICCIA MESSINA

Diritto all'oblio e alla portabilità di dati da un social network. E ancora diritto ad essere informati in caso di violazione dei dati personali. Queste alcune delle novità del Regolamento europeo sulla privacy, approvato ieri dal Parlamento Ue, che, tempo due anni manderà in soffitta il codice della privacy italiano e le leggi sulla riservatezza degli stati Ue. Sulla privacy, dunque, si riparte a tinte europee e con una legislazione uniforme in tutto il vecchio continente. Nel pacchetto privacy c'è anche una direttiva sui trasferimenti di dati a fini giudiziari e di polizia. Si applica ai trasferimenti di dati attraverso le frontiere all'interno dell'Unione europea e stabilisce, per la prima volta, norme minime per il trattamento dei dati a fini di polizia all'interno di ogni Stato membro. Il regolamento, che aggiorna la direttiva risalente al 1995, riguarda anche la disciplina dell'organizzazione degli adempimenti per le imprese e per le pubbliche amministrazioni. Scompariranno adempimenti formali, come la notificazione dei trattamenti al Garante. Ma saranno da curare adempimenti di tutela sostanziale, come la valutazione dell'impatto dei trattamenti sulla protezione dei dati e la eventuale verifica delle prescrizioni da adottare presso le autorità di controllo. E il tutto si realizzerà sotto l'occhio del responsabile della protezione dei dati: figura da nominare obbligatoriamente nelle p.a. e nelle imprese, se impegnate nel trattamento dei dati delle persone su larga scala. Riformulato l'apparato sanzionatorio, calcolato in misura percentuale sul fatturato delle aziende (così da diventare veramente efficace verso colossi planetari).

Portabilità dei dati. All'interessato viene riconosciuto il diritto di ottenere la restituzione dei propri dati personali trasmessi ad un'azienda o a un servizio online e trasmetterli ad altri (social network, fornitori di servizi internet, fornitori di streaming online ecc.).

Sportello unico. L'interessato può rivolgersi al Garante del proprio paese per segnalare eventuali violazioni, qualunque sia il luogo in cui il trattamento è effettuato.

Oblio. Il regolamento codifica il diritto dell'interessato di chiedere ai motori di ricerca di deindicizzare una pagina web o chiedere ad un sito web di cancellare informazioni.

Profilazione. Il regolamento sancisce il diritto a non subire profilazioni (trattamenti automatizzati) a propria insaputa.

Consenso. Il regolamento pretende che il consenso dell'interessato sia effettivo e inequivocabile. Può essere formulato, ad esempio, mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Questo può avvenire anche mediante selezione di un'apposita casella in un sito web, ma non è consenso il silenzio, l'inattività o la preselezione di caselle.

Valutazione d'impatto. In casi specifici, come il ricorso a tecnologie a rischio per i diritti delle persona, il trattamento deve essere testato con una valutazione d'impatto privacy ed eventualmente con consultazione preventiva del garante.

Privacy by design e by default. Il regolamento impone di progettare sistemi e applicativi, di regola tarati sul principio dell'uso minimo e indispensabili dei dati personali. Si devono adottare d esempio sistemi di pseudonomizzazione oppure misure e sistemi che abbiano come impostazione predefinita solo l'uso dei soli dati necessari per una certa finalità.

Sicurezza. Scomparsi adempimenti burocratici, viene esaltato un approccio basato sull'analisi dei rischi e sull'adeguatezza delle misure di tutela. Utile l'adesione a sistemi di certificazione e codici di condotta.

Violazione dati. Si estende a tutti la regola della notifica di violazione dei dati personali al garante e all'interessato (a quest'ultimo in caso di rischio elevato per i suoi diritti).

Data protection officer. È una nuova figura di riferimento per imprese e p.a., per utenti e clienti ed è l'interfaccia per le autorità garanti. Nel settore privato dovrà essere nominato in caso di trattamenti di dati su larga scala o di monitoraggio sistematico degli interessati su larga scala.

Codici etici e certificazioni. Codici di autoregolamentazione e ricorso alle certificazioni dei trattamenti e sono incoraggiati. Si tratta di «bollini blu», di cui si terrà conto nelle verifiche, ispezioni e anche nella determinazione delle sanzioni.

Direttiva dati giudiziari. Le nuove norme mirano a proteggere gli individui, vittime, criminali o testimoni, stabilendo diritti chiari e limitazioni al trasferimento dei dati personali a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, compresa la protezione delle persone e la prevenzione di minacce alla sicurezza pubblica. Allo stesso tempo, il testo mira a facilitare la cooperazione giudici-polizia.

Prossime tappe. Ora tocca al Consiglio Ue prendere atto formalmente dell'approvazione del pacchetto da parte del Parlamento. Seguirà la pubblicazione in *Gazzetta ufficiale dell'Unione europea*, prevedibilmente entro fine giugno. Il Regolamento entrerà in vigore 20 giorni dopo la pubblicazione e, dopo due anni, le sue disposizioni saranno direttamente applicabili in tutta l'Ue. Gli Stati membri avranno due anni per recepire le disposizioni.

Reazioni. Secondo **Antonello Soro**, presidente Garante privacy, regolamento e direttiva «si pongono anche come una sfida sia per le Autorità garanti sia per imprese, soggetti pubblici, liberi professionisti chiamati ad un ruolo di grande rilievo e responsabilità».

Le novità in arrivo

Portabilità dei dati	Diritto al trasferimento dati da un titolare a un altro (ad esempio, tra social netwok)
Oblio	Diritto a deindicizzare pagina web o informazioni in rete
Profilazioni	Stop a trattamenti automatizzati inconsapevoli
Consenso	Espresso e inequivoco (non va bene la preselezione di caselle)
Valutazione di impatto e sicurezza	Analisi dei rischi derivanti dal trattamento
Privacy by design	Progettare trattamenti conformi al regolamenti
Privacy by default	Impostazioni predefinite sul trattamento minimo di dati
Violazione dati	Diritto di venire a conoscenza della violazione (hackering) dei propri dati personali
Responsabile protezione dati	Nomina obbligatoria per p.a. e imprese che trattano dati su larga scala
Codici etici e certificazioni	Incentivata l'adesione che porta benefici in caso di valutazione della legittimità dei trattamenti (anche in sede ispettiva e sanzionatoria)

CORRIERE DELLA SERA

Data 17-04-2016
Pagina 27
Foglio 1

NO AL MONOPOLIO DEI SOCIAL LIBERALIZZIAMO I NOSTRI DATI

Molti commentatori si sono finalmente accorti che Facebook, Google e gli altri Over the Top sono ormai diventati monopoli incontrollabili, che sfuggono alle regole cui sottostanno le altre aziende. Le «ambizioni imperiali» di Zuckerberg, ha scritto l'*Economist*. Fino a oggi però il tema è stato affrontato quasi esclusivamente in chiave di privacy, cioè contestando che i big della Rete facciano commercio dei nostri dati personali. Ma non è solo usando la leva della privacy che le superpotenze digitali verranno ridotte a più miti consigli: anche se una tutela più efficace dei dati personali (come il Regolamento in discussione a Bruxelles) non può che fare bene. La maggioranza degli internauti tuttavia, come spesso ricorda lo stesso Zuckerberg, baratta volentieri il suo «privato» con i servizi che riceve in cambio.

No. Gli Over the Top possono essere ricondotti alle regole comuni soltanto se i dati personali, di cui oggi si appropriano senza l'obbligo di condividerli con i concorrenti, vengono sottratti al loro dominio esclusivo. Si può pensare a una «liberalizzazione dei dati» in due fasi. La prima è quella di introdurre la portabilità dei dati personali da un provider all'altro. Oggi, se voglio, posso chiudere il mio profilo Facebook: ma non portare via le informazioni che mi riguardano.

La seconda fase sarebbe una diretta conseguenza della prima: introdurre la possibilità di negoziare l'uso dei dati personali in cambio di vantaggi economici. Ad esempio sconti, offerte speciali, insomma condivisione, per il consumatore, dei benefici pubblicitari che fanno ricchi gli Over the Top. Con la facoltà, se non ottengo ciò che chiedo, di cambiare fornitore. Con la liberalizzazione del 1998, le compagnie telefoniche sono state forzate ad aprire le reti ai concorrenti, con forti cali di prezzi per gli abbonati. Forse è venuto il momento di mettere in discussione anche il «monopolio dei dati», aprendolo a una vera competizione e a nuovi soggetti.

Edoardo Segantini


DESTRA E SINISTRA
L'EROSIONE DI IDENTITÀ
CHE OMOLOGA LA POLITICA

NO AL MONOPOLIO DEI SOCIAL
LIBERALIZZIAMO I NOSTRI DATI

UN QUESITO DA DIVIDERE
I RADICALI SI MOBILITANO

Il Sole 24 ORE nòva 24

Data 17-04-2016
Pagina 1
Foglio 1

Digitale | Etica | Informazioni

Il governo umano delle tecnologie

Luciano Floridi: «Vietare la pubblicità online» Così si ferma il commercio dei dati e il potere di scelta resta ai cittadini, agli utenti

di **Chiara Somajni**

La proposta del filosofo Luciano Floridi è radicale: vietare la pubblicità online. «Così staccheremmo il cordone, metteremmo le basi per un mercato competitivo, obbligando aziende come Google e Facebook a rivedere il loro modello di business»: gli utenti, invece di beneficiare dell'odierno "regalo", solo apparentemente gratuito in cambio della loro attenzione e dei loro dati dovrebbero pagare per i servizi che intendono usare, e si orienterebbero verso quelli migliori. Direttore della ricerca e professore di filosofia ed etica dell'informazione all'Oxford Internet Institute, membro del Google Advisory Council e da gennaio dell'Ethics Advisory Group europeo, Floridi vede in quest estrema ipotesi normativa una risposta possibile alla concentrazione di potere raggiunto da un numero ristretto di società americane. È la legge a suo avviso l'unico baluardo e i precedenti dell'industria del tabacco, della farmaceutica e dell'alimentare ne dimostrano l'efficacia.

I *frightful five*, i terribili cinque, come li chiama il New York Times (Google, Microsoft, Apple, Amazon Facebook), stanno diventando i provider di default di infrastrutture essenziali, in finanza, nella salute, nell'educazione, osserva il critico Evgeny Morozov. Una posizione dominante problematica per il mercato, che danneggia anche i consumatori e l'innovazione. Robert Bernard Reich, docente di Amministrazione e politiche pubbliche a Berkeley, ricorda un rapporto del 2012 su Google realizzato dallo staff della Commissione federale americana per il commercio, la cui raccomandazione di intraprendere un'azione legale contro la società per abuso di posizione dominante non venne raccolta. Cosa alquanto insolita, sottolinea Reich, ma che trova qualche spiegazione nell'attività di lobbying: negli Stati Uniti gli investimenti volti a influenzare i decisori politici da parte delle società tecnologiche competono con quelli dell'industria militare e petrolifera. «Ha potere chi può influenzare le scelte e i comportamenti umani - dice Floridi -. C'è il potere visibile, del monarca, del politico, del dittatore, e quello che di solito è chiamato grigio, il potere di influenzare chi esercita pubblicamente il potere: molto più interessante, perché non è né legittimato né *accountable*. Questo era esercitato in passato da chi aveva i mezzi di produzione, gli industriali. Lo definisco il potere sulle cose. Nel frattempo era già emerso il potere sulle informazioni sulle cose, esercitato dalla stampa, il cui culmine è rappresentato dallo scandalo Watergate. Oggi siamo arrivati a una terza fase: a prevalere è chi gestisce la produzione delle informazioni sulle cose».

Le implicazioni sono di ordine politico, sociale, etico. Quanto pregnanti e attuali lo evidenziano casi di conflitto tra i diritti alla privacy, alla libertà di espressione e alla sicurezza, tra interessi privati e interesse pubblico. Il contenzioso tra Apple e Fbi, ad esempio: un braccio di ferro che ridotto ai minimi termini può essere visto come il tentativo della società californiana di affermare la propria autonomia, e il proprio potere, rispetto allo Stato, ergendosi a difesa degli interessi degli individui. Con quale legittimazione e quali limiti vadano posti al diritto alla privacy dei cittadini è oggetto di discussione. Ci si schiera a favore di Apple, ma contro chi si è visto esposto dai Panama Papers, facendo una distinzione tra *good guys* e *bad guys* difficile da argomentare dal punto di vista del diritto, osserva l'avvocato David Allen Green sul Financial Times: in entrambi i casi, c'è un provider commerciale che offre un servizio per il quale i clienti si aspettano la sicurezza dei dati cui si contrappone un interesse pubblico. Sul piano della legittimazione, un potere per sua natura non *accountable*, basato su contratti poco comprensibili all'utenza e spesso modificati, il cui perno è la fiducia. Ma se Facebook può indurre gli utenti ad andare a votare, chi assicura che il suo invito non sia rivolto a un target di parte, come paventa Martin Moore, direttore del Media Standards Trust? L'esperimento condotto da Facebook nel 2012 per verificare l'influenzabilità dell'umore degli utenti è di per sé un inquietante precedente. Per Floridi c'è da attendersi che il contenzioso tra *big tech* e autorità pubblica salga di grado, fino a investire i governi eletti.

In che misura società tecnologiche dalle ambizioni imperiali, per riprendere la penultima copertina dell'Economist, abbiano interesse a difendere la privacy dei cittadini è pure questione dubbia, considerato che sul riuso dei dati a fini commerciali si fonda il loro successo economico. Per Morozov ci vorrebbe una Bbc dei dati, un servizio pubblico dove raccogliere i contenuti scollegati dagli identificativi personali, a tutela degli utenti e a beneficio dell'innovazione e della concorrenza. L'emergere di soggetti come Telegram, che sfida WhatsApp/Facebook garantendo privacy e sicurezza, va in questa direzione.

«In gioco - sostiene Floridi - c'è il progetto umano: vogliamo che sia politico-sociale o commerciale?». Al di fuori degli Usa la resistenza al monopolio di *big tech* è più marcata, Europa in testa, con risultati come il diritto all'oblio imposto a Google o la legge per la protezione dei dati personali appena approvata dal Parlamento europeo, apprezzata da Floridi come «un passo fondamentale, che spero contribuirà a ricollocare le persone e i loro diritti al centro del progetto socio-politico, offrendo all'Europa la leadership etico-legale in questo ambito». Ma è disarmante, osserva Floridi, che sia proprio l'Europa a definire i cittadini *data subjects*, invece che persone: della portata culturale che questa deviazione linguistica tradisce, ormai neppure ci rendiamo conto.

Il Sole 24 ORE

Data 17-04-2016
Pagina 11
Foglio 1

Crossroads

MERCATO EUROPEO DEI DATI PROTETTI

di **Luca De Biase**

Dopo una lunga gestazione, il Parlamento europeo ha approvato il regolamento sulla protezione dei dati. E forse ha aperto una nuova epoca di opportunità per l'industria digitale europea. L'unificazione delle regole consente alle imprese di operare senza troppi patemi nei diversi paesi europei. In questo quadro, l'Europa si è data norme identitarie, come il diritto all'oblio, la garanzia dell'anonimato, la privacy by design che possono costituire un fondamento decisivo per lo sviluppo della civiltà digitale nel continente che, per la sua dimensione, potrebbe influenzare lo stesso sviluppo civile globale. Gli americani, in effetti, erano partiti molto scettici sulla questione della privacy. I leader di Google e Facebook anni fa trattavano esplicitamente la privacy come una faccenda vecchia e superata. Ma i loro clienti, soprattutto dopo le rivelazioni di Edward Snowden sulla sorveglianza di massa operata dall'Nsa, hanno maturato una nuova sensibilità in materia. E anche sulla scorta dei valori europei, Apple e Microsoft, poi persino Google e Facebook, hanno imparato a rivalutare la privacy dei loro utenti. Costruendo strumenti che appaiono votati a garantirla, almeno nei confronti delle autorità pubbliche. L'Europa però chiede anche privacy nei confronti delle aziende private. E su questo punto le grandi piattaforme americane che vivono di pubblicità hanno ancora qualcosa da imparare dalla civiltà europea. Che a questo punto potrebbe finalmente avere posto le premesse per lanciarsi nella costruzione di piattaforme europee rispettose dei diritti umani, interoperabili, civiche. Non per sostituire i successi americani, ma per creare una nuova dimensione nella vita digitale, adatta al contesto dell'internet delle cose, della robotica, dell'intelligenza collettiva. Il mercato interno europeo si è strutturato un po' meglio, questa settimana. E le opportunità sono cresciute. La lotta per i diritti umani in rete non è vinta. La neutralità della rete è ancora in pericolo in Europa. E l'eccesso di sorveglianza non è scongiurato. Ma un passo avanti è stato compiuto.


nòva 24

Il governo umano delle tecnologie

L'evoluzione imprevista dell'ufficio

Guerre d'Arabia

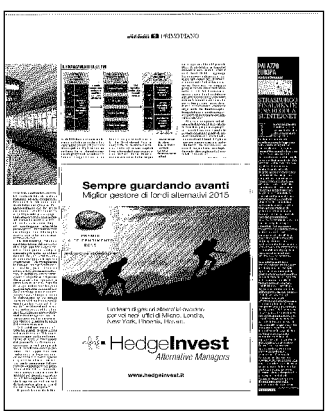
la Repubblica A&F AFFARI&FINANZA

Data 18-04-2016
Pagina 9
Foglio 1

STRASBURGO FINALMENTE UNA REGOLA SU INTERNET

Andrea Bonanni

La notizia è passata quasi inosservata, sovrastata dal fatto che il Parlamento europeo ha finalmente approvato la schedatura dei passaggeri sui voli extra Ue (Pnr). Ma nel corso della stessa sessione, l'assemblea ha anche dato il via libera ad un pacchetto di misure che regola la tutela della privacy e il trattamento dei dati personali su Internet. Le nuove regole sostituiscono una direttiva varata nel 1995, quando la rete era ancora ben lontana dall'aver acquisito l'importanza e l'invadenza attuali, e sono il frutto di uno dei processi decisionali più complessi della legislazione europea. Basti pensare che i negoziati tra Commissione, Consiglio e Parlamento sono cominciati nel 2012 e che il dibattito nelle commissioni parlamentari interessate ha visto la presentazione di quattromila emendamenti. La nuova normativa prevede che i dati personali non possano essere trattati senza un consenso esplicito dagli interessati, che può essere revocato in qualsiasi momento. Inoltre, in alcuni casi, garantisce il diritto all'oblio, cioè alla cancellazione delle proprie pagine sui social media, soprattutto per i minori. Altra innovazione importante è la «portabilità» dei propri dati personali che, su richiesta dell'interessato, potranno essere trasferiti automaticamente da un provider ad un altro. In questo modo si potrà, per esempio, aprire un nuovo account di posta elettronica trasferendovi automaticamente sia il proprio indirizzario sia le mail del vecchio account. Vengono stabiliti limiti al «profiling» degli utenti a fini commerciali. Infine i gestori dei dati avranno l'obbligo di avvertire gli interessati qualora le informazioni che li riguardano siano state piratate. Insieme con queste regole per la tutela della privacy, il Parlamento ha anche approvato una direttiva che regola la trasmissione e lo scambio dei dati personali da parte delle forze di polizia, dei servizi e delle magistratura. Da una parte vengono stabiliti limiti al loro utilizzo, dall'altra si definiscono parametri comuni che rendano più rapido e agevole lo scambio di informazioni tra un Paese e l'altro. Le resistenze per approvare le nuove norme sono state molto forti, soprattutto all'interno del Consiglio per le posizioni divergenti dei vari governi. Alla fine la situazione si è sbloccata solo quando il Parlamento ha posto come condizione per l'approvazione del registro dei passeggeri aerei, che il Consiglio desse il proprio via libera al pacchetto sulla protezione dei dati personali.



Il Messaggero

Data 18-04-2016
Pagina 14
Foglio 1

L'intervento/

Indagini informatiche, quei limiti che vanno fissati

Paolo De Angelis

Il Grande Fratello è tra noi e si chiama captatore informatico, strumento che consente di acquisire ogni dettaglio della vita privata della vittima che tecnicamente è chiamato "bersaglio", con raggelante realismo; mediante un virus autoinstallante indirizzato ai dispositivi elettronici (compresi cellulari e tablet), la vita del "bersaglio" viene registrata in diretta, con una potenza invasiva totale, senza possibilità di difesa. L'immissione del virus avviene in modo occulto e il suo funzionamento non è nemmeno rilevabile ai normali controlli; da quel momento (basta aprire una mail o cliccare su un allegato) la privacy, la riservatezza, la stessa vita privata diventano concetti senza più senso per chi, a sua insaputa, viene costantemente controllato.

Il captatore ascolta i dialoghi, legge la rubrica, copia le mail, pedina gli spostamenti, riprende i movimenti (si può impossessare anche delle telecamere del dispositivo infettato); insomma, altro che truman show, nemmeno Orwell aveva previsto un simile annullamento delle libertà individuali, col semplice controllo degli apparecchi informatici. Va detto, per mettere in chiaro le cose, che se il captatore viene installato da un privato (come nel caso di un marito geloso per sapere cosa faccia la moglie in sua assenza oppure di un datore di lavoro per venire a conoscenza dei movimenti dei propri dipendenti), si tratta di un grave reato che viola il divieto di intromissione nella vita privata e la tutela della riservatezza. Ma il problema riguarda un aspetto ben più significativo e rilevante, quando cioè il captatore informatico è utilizzato per le indagini giudiziarie.

Da quando questi particolari programmi sono stati creati e perfezionati, la polizia giudiziaria e la magistratura hanno iniziato a farne uso, come nuova forma di intercettazione; il mafioso, il politico corrotto, il terrorista vengono sottoposti alla captazione, così ogni aspetto della loro vita viene conosciuto e scandagliato, per ottenere prove schiaccianti a carico. Tutto bene allora? Non proprio: il tema delle libertà individuali e dei diritti fondamentali è delicato e richiede la massima cautela poiché le deroghe ai principi, anche quando avvengono per finalità di interesse generale come il contrasto alla criminalità, rischiano di aprire crepe nella tutela della persona e nella stessa visione costituzionale delle libertà personali. La questione, ridotta nelle sue linee essenziali, è se la lotta al crimine consenta di introdursi nella vita privata degli indagati senza alcun limite o se le libertà individuali siano inviolabili, anche di fronte agli accertamenti della magistratura; in definitiva, se lo Stato, anche quando la sua azione è legittima e giustificata come nel caso di indagini giudiziarie, abbia un potere illimitato di conoscenza e di intromissione nella vita del cittadino.

Non è una questione di poco conto: si può sostenere che per assicurare alla giustizia criminali pericolosi non ci siano limiti negli accertamenti e quindi la libertà individuale può cedere il passo alla tutela degli interessi collettivi. Una sorta di moderno fine che giustifica i mezzi: ma siamo sicuri che possa essere davvero così? La nostra Costituzione riconosce e fissa libertà fondamentali inviolabili, senza limiti, se non nei casi previsti dalla legge: e nessuna legge ha mai disciplinato i captatori informatici. Nelle sentenze che si sono occupate di questi casi, il captatore informatico viene considerato alla stregua di una intercettazione di tipo ambientale, come una microspia installata in una casa o in un ufficio ma c'è una bella differenza rispetto a questi casi "classici" perché nel caso del captatore la cimice è installata non in un luogo ma su una persona (o meglio, sul suo dispositivo mobile, oramai compagno inseparabile di chiunque) e funziona in ogni momento, in ogni ambiente, per ogni occasione (quando delinque ma anche nella più privata intimità). Insomma, un potentissimo mezzo di intrusione, praticamente senza limiti. Il 10 marzo scorso la Corte di Cassazione si è rivolta alle Sezioni Unite, proprio per sapere se la captazione informatica sia una forma legittima di intercettazione e se i suoi risultati siano utilizzabili nei processi. In attesa della sentenza, è bene riflettere sul problema e chiarire che, al di là della questione puramente tecnica, sono in gioco valori costituzionali, come la Germania, sin dal 2008, ha perfettamente compreso, dichiarando incostituzionale la captazione informatica. Prevarrà l'interesse dello Stato alle indagini criminali oppure l'interesse individuale alle libertà fondamentali? Lo deciderà la Suprema Corte ma sarebbe molto meglio se su una questione così cruciale intervenisse il Parlamento: solo una legge, che oggi manca del tutto, può stabilire un equilibrato bilanciamento tra esigenze così importanti e non pienamente compatibili tra loro. Non è soluzione di scarso rilievo, anzi: si tratta di delineare i confini della democrazia.

Sostituto procuratore presso il Tribunale di Cagliari

Il Messaggero

Data 28-04-2016
Pagina 17
Foglio 1

Privacy, il Garante: Facebook deve bloccare i "fake"

IL CASO

ROMA Facebook dovrà comunicare a un proprio utente tutti i dati che lo riguardano, informazioni personali, fotografie, post, anche quelli inseriti e condivisi da un falso account, il cosiddetto "fake". Non solo: la società di Menlo Park dovrà bloccare il "fake" ai fini di un eventuale intervento da parte della magistratura. Lo ha stabilito il Garante per la protezione dei dati personali nella sua prima pronuncia nei confronti del colosso web, nella quale afferma la propria competenza a intervenire a tutela degli utenti italiani. A riferirlo è la Newsletter del Garante.

Il social network dovrà, inoltre, fornire all'iscritto, in modo chiaro e comprensibile, informazioni anche sulle finalità, le modalità e la logica del trattamento dei dati, i soggetti cui sono stati comunicati o che possano venirne a conoscenza.

Il Garante ha accolto il ricorso di un iscritto a Facebook che si era rivolto all'Autorità dopo aver interpellato il social network e aver ricevuto una risposta ritenuta insoddisfacente. L'iscritto lamentava di essere stato vittima di minacce, tentativi di estorsione, sostituzione di persona da parte di un altro utente di Facebook, il quale, dopo aver chiesto e ottenuto la sua "amicizia", avrebbe inizialmente intrattenuto una corrispondenza confidenziale, poi sfociata nei tentativi di reato. Il ricorrente sosteneva, inoltre, che il "nuovo amico", visto il suo rifiuto di sottostare alle richieste di denaro, avrebbe creato un falso account, utilizzando i suoi dati personali e la fotografia postata sul suo profilo, dal quale avrebbe inviato a tutti i contatti Facebook dell'interessato fotomontaggi di fotografie e video gravemente lesivi dell'onore e del decoro oltre che della sua immagine pubblica e privata.

R.I.

CHIESTA AL SOCIAL PIÙ TRASPARENZA SUI DATI PERSONALI COMPRESI QUELLI MESSI IN RETE CON FALSI ACCOUNT


Roma, rischia la vita per una minerale al bar

Privacy, il Garante: Facebook deve bloccare i "fake"

la Repubblica

Data 29-04-2016
Pagina 8
Foglio 1

>L'ANALISI

GIANLUCA DI FEO

Cyber-sicurezza, il ritardo dell'Italia

LA CYBERSECURITY è una cosa seria. Bisogna proteggere l'intera rete del Paese e vigilare su tutte le comunicazioni, bloccando qualunque intrusione illecita. È il nuovo fronte di quelle "guerre ibride", combattute in una zona grigia senza confini e senza esclusione di colpi. In Italia se ne discute da tempo e Matteo Renzi sembra intenzionato ad affidare la supervisione della materia al suo amico del cuore, Marco Carrai: nel Consiglio dei ministri di oggi potrebbe essere decisa la nomina, con una posizione di consulente di Palazzo Chigi e una piccola struttura ad personam.

Anche in Germania si sono posti il problema e due giorni fa hanno annunciato la loro risposta. Poiché i grandi attacchi ai sistemi cibernetici - quelli che possono bloccare le linee ferroviarie, mandare in tilt la rete elettrica o azzerare i computer di un'azienda -, sono sempre più simili ad azioni di natura militare, Berlino ha deciso di affidare il compito di impedirli al ministero della Difesa. Il piano presentato da Ursula von der Leyen, la prima donna al vertice del dicastero, crea una nuova branca delle forze armate, con un organico di 13.500 tra militari e tecnici civili. Il Cir, CyberInformationsRaum, avrà sede a Bonn e si occuperà di vigilare sull'intera sapienza tecnologica della nazione. È previsto l'investimento di un miliardo di euro e alla guida ci sarà un generale a due stelle.

E da noi? Siamo fermi al rapporto "Cyber minacce e sicurezza", scritto sei anni fa dal Comitato parlamentare di controllo sull'intelligence, che raccomandava «al governo di dotarsi di un impianto strategico-organizzativo che assicuri una leadership adeguata e predisponga chiare linee politiche per il contrasto alle minacce e il coordinamento tra gli attori interessati». Marco Carrai è la figura che può garantire questa leadership? L'amico del premier non è laureato, ma vanta un trascorso di consultant al Mit di Boston e una recente attività imprenditoriale proprio nel settore della sicurezza telematica. Mentre dopo mesi di audizioni e studi, il Comitato parlamentare nel 2010 aveva ipotizzato una linea diversa, consigliando di affidare la missione all'organismo che dirige i nostri servizi segreti: «Il Dis appare il riferimento istituzionale più idoneo». Già, ma quella relazione era stata scritta dal senatore Francesco Rutelli e voluta dal presidente del Copasir Massimo D'Alema: difficile che Renzi la prenda in considerazione.


La polemica
Manager e politici con vecchi cellulari in fuga dal virus-spia degli smartphone

LA STAMPA

Data 29-04-2016
Pagina 14
Foglio 1

Anche on line contano i diritti

Uguaglianza e democrazia devono valere nella dimensione digitale

ANNA MASERA

Accesso, cultura, uguaglianza, privacy, identità, anonimato, cittadinanza, oblio, sicurezza, democrazia: sono le dieci parole chiave che rappresentano i nostri diritti fondamentali se vogliamo dirci cittadini della Rete. Perché, come dice Stefano Rodotà, Internet non è un luogo vuoto di regole: al contrario, è sempre più regolata da Stati invadenti e imprese prepotenti, che con il pretesto della sicurezza e agevolati dagli strumenti digitali controllano le persone in modi sempre più diffusi e penetranti. E' necessario che i cittadini acquisiscano consapevolezza dei loro diritti online: dopotutto l'aspirazione alla libertà è stata una ragion d'essere per gli inventori del cyberspazio. In occasione dell'Internet Day, il ministero dell'Istruzione ha previsto su questo tema, fondamentale per l'educazione al digitale, un laboratorio con gli studenti delle superiori. Farà da bussola la Dichiarazione dei diritti in Internet approvata dalla Camera il 3 novembre, spiegata nella guida *Internet, i nostri diritti* (Laterza). Gli insegnanti sul sito del Miur troveranno le informazioni e gli esercizi proposti per uso didattico con l'illustrazione attraverso immagini e video evocativi delle parole chiave.

Che significa non poter accedere a Internet oggi? Come si possono far valere l'uguaglianza e la democrazia nella dimensione digitale? Come preservare il proprio diritto alla privacy? Siamo prima persone o prima utenti da profilare? Come esercitare la libertà online? Siamo cittadini anche sulle piattaforme digitali? Quando è giusto chiedere a Internet di dimenticare? Come garantire la sicurezza online? E infine in rete chi comanda, chi decide le regole e chi le fa rispettare? Siamo davanti a una delle sfide più complesse del nostro tempo. E' bene che se ne parli a scuola.

@annamasera


30 aprile 1996
L'Italia arriva (tardi) in rete
Quando l'establishment rideva del web
Anche on line contano i diritti

Il Sole 24 ORE

Data 09-05-2016
Pagina 1
Foglio 1 / 2

La tutela dei dati
VERSO REGOLE UGUALI PER TUTTI

La transizione. Ai Paesi membri due anni per adeguarsi alle novità che saranno direttamente efficaci dal 25 maggio 2018

Privacy, staffetta Italia-Europa

Il nuovo regolamento europeo sostituisce dopo vent'anni le norme nazionali

di **Antonello Cherchi**

Vent'anni fa l'Italia scopriva la privacy. Nel senso che, su input dell'Europa, si dotava di regole per proteggere i dati personali. Gli italiani in tutto questo tempo hanno scoperto e apprezzato il valore della riservatezza.

Nel frattempo hanno preso sempre più piede internet e tutto ciò che ne consegue. E le privacy nazionali hanno mostrato la corda. Per questo si preparano a passare il testimone al nuovo regolamento Ue, che detta misure di protezione dei dati uguali per tutta l'Unione. Avranno due anni per adeugarsi, prima che il 25 maggio 2018 la privacy sia solo europea.

Maggio è il mese odoroso cantato da Leopardi, ma, più prosaicamente, anche quello della privacy. Tutto è accaduto a maggio. Diciannove anni fa, di questi giorni - esattamente l'8 maggio - faceva il suo debutto la prima legge italiana sulla tutela dei dati personali, che in realtà quest'anno compie venti anni, perché ha visto la luce nel 1996. Portava il numero 675 e come la sua "sorella minore" - la legge 676 dello stesso anno, che dava al Governo la possibilità di intervenire per correggere o integrare la prima - prendeva spunto da un input europeo. Era stata, infatti, la direttiva 95/46 a dire a ogni Paese della Ue di recepire le norme a protezione della privacy.

Ed è sempre l'Europa a ritornare in questi giorni sull'argomento per aggiornare in modo significativo quanto dettato nel 1995 e recepito dal nostro Paese l'anno successivo. Al termine di un sofferto e lungo iter legislativo, la Ue ha riscritto le regole sulla privacy. Lo ha fatto con il regolamento 2016/679, pubblicato qualche giorno fa sulla Guce, la Gazzetta dell'Unione. La nuova normativa entrerà in vigore il 24 maggio e non avrà bisogno di recepimento. Ci sarà solo un biennio di interregno, durante il quale i Paesi membri sceglieranno come adeguarsi e in che modo inglobare il nuovo provvedimento nelle leggi nazionali. Il 25 maggio 2018, il regolamento diventerà operativo in tutta la Ue, soppiantando le disposizioni interne di ciascuno Stato che si sovrappongono alle nuove regole. Nel nostro caso, a farne le spese sarà il Codice della privacy (il decreto legislativo 196/2003).

Ma non si tratta dell'unica novità in materia di riservatezza personale arrivata in questo maggio. Nella stessa Gazzetta che ha ospitato il regolamento sono state, infatti, pubblicate anche due direttive: la prima sulla tutela dei dati personali nell'ambito delle attività investigative e un'altra sulla banca dati del Pnr (il Passenger name record), cioè le informazioni (per esempio, la data del viaggio, i recapiti telefonici, la mail, l'itinerario, le modalità di pagamento, il posto assegnato, il tipo di bagaglio) di chi vola da e per l'Europa.

Sempre di privacy, dunque, si parla. Per quanto in quest'ultimo caso - a differenza del regolamento e della prima direttiva - più che di protezione dei dati, si tratta di "intrusione" nelle informazioni personali, della loro raccolta massiva nel nome della lotta al terrorismo. Ci sono voluti anni per arrivarci, ma le recenti vicende francesi e belghe hanno spazzato via le ultime resistenze.

È sempre l'urgenza della contemporaneità a scrivere l'agenda della privacy dei nostri giorni: gli attentati hanno costretto al Pnr, le nuove tecnologie e internet hanno dettato il nuovo regolamento. Nell'epoca di Google e Facebook occorrono misure comuni di protezione dei dati. Serve una disciplina «uniforme e armonizzata tra tutti gli Stati membri» che elimini - ha commentato il Garante italiano Antonello Soro - «le numerose asimmetrie che si erano create nel tempo».

Per quanto la matrice fosse la stessa - la direttiva 95/46 - ogni Paese l'aveva, infatti, declinata e applicata a modo proprio. Una frammentazione di norme che pure non ha ostacolato il formarsi di una coscienza collettiva del valore delle nostre informazioni personali.

È quanto accaduto nel quasi ventennio di privacy italiana. Quando la legge 675 fece capolino, la convinzione diffusa era che "privacy" fosse uno sfoggio per dire altrimenti "riservatezza". Niente molto di più. A partire da quell'8 maggio di tanti anni fa, la consapevolezza dell'importanza delle informazioni personali è pian piano cresciuta. Anche grazie al lavoro del Garante. Una rilevazione del Censis del 2013 ha registrato che il 96% dei cittadini ritiene la riservatezza un diritto inviolabile e il 93% teme di veder attaccata la propria privacy online. Preoccupazione che si accompagna a una richiesta di regole di protezione più stringenti (lo chiede il 53% degli intervistati).

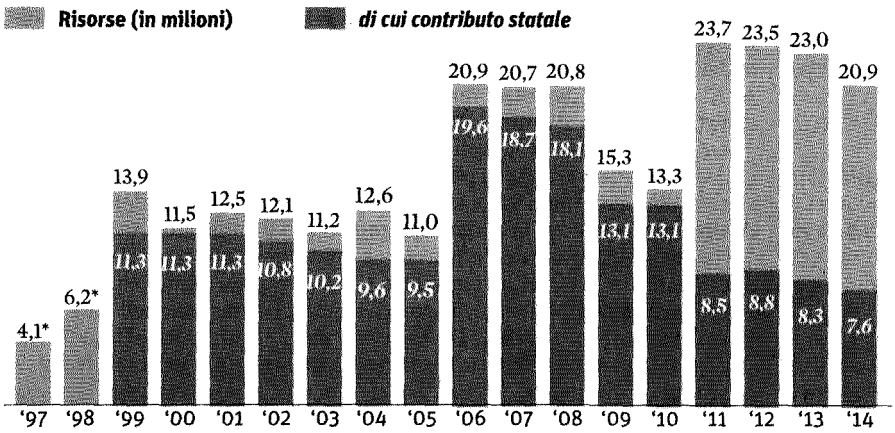
Il nuovo regolamento risponde a queste esigenze: disposizioni comuni per dare ai cittadini maggiori tutele e alle imprese più facilità nell'applicarle. Uno strumento più efficace per difendersi, per esempio, da chi ci chiede un consenso indifferenziato all'uso dei nostri dati come condizione per accedere a un servizio. Accade sempre più spesso online. Ora, però, grazie al regolamento, si può invocare anche il diritto all'oblio, ovvero chiedere e ottenere la cancellazione dei nostri dati.

Il passaggio di testimone è appena iniziato.

FRONTE COMUNE
Dal 1996 a oggi si è fatta strada la consapevolezza del valore delle informazioni personali ma ora servono misure comuni a tutti gli Stati

A guardia della riservatezza

Da debutto ai giorni nostri: le risorse finanziarie per far funzionare l'ufficio del Garante



* Nel 1997 e 1998 le risorse e il contributo statale coincidono. Dal 2011 la parte preponderante delle risorse, oltre i contributi statali, è rappresentata da trasferimenti di altre Autorità indipendenti

Fonte: Garante della privacy

LE FORZE IN CAMPO
Il personale di cui dispone il Garante

	In servizio		A contratto	Totale
	Di ruolo	Fuori ruolo		
1998	3	36	-	39
1999	3	42	-	45
2000	42	9	-	51
2001	42	16	11	69
2002	59	17	15	91
2003	59	16	18	93
2004	67	15	12	94
2005	74	8	14	96
2006	78	7	9	94
2007	85	5	13	103
2008	85	9	13	107
2009	101	10	15	126
2010	99	10	16	125
2011	99	10	20	129
2012	101	7	18	126
2013	101	8	18	127
2014	113	4	8	125

Nota: nel 1998 e 1999 non c'era personale di ruolo, ma solo comandati e personale fuori ruolo
Fonte: Garante della privacy

L'ATTIVITÀ
Alcuni ambiti di intervento del Garaante

	Segnalazioni e reclami	Ricorsi decisi	Ispezioni
1998	7.000*	—	n.r.
1999	1.946	125	n.r.
2000	3.661	158	20
2001	4.295	169	18
2002	7.550	390	35
2003	7.109	608	69
2004	6.391	731	10
2005	1.269	634	4**
2006	2.998	435	9
2007	3.084	316	24
2008	3.272	321	34
2009	3.493	360	30
2010	3.359	349	8
2011	4.022	257	8
2012	4.592	233	14
2013	4.393	222	411***
2014	4.170	306	385

Note: n.r.= non rilevato -* Compresi i quesiti -
** Effettuate, dal 2005 al 2012, in base all'articolo 158 del Codice della privacy - *** Effettuate, nel 2013 e 2014, In base agli articoli 157 e 158 del Codice della privacy
Fonte: Garante della privacy

CORRIERE ECONOMIA

Data 16-05-2016
Pagina 6
Foglio 1

Il nuovo approccio del Garante che verrà illustrato nella Relazione annuale del 28 giugno

La privacy? Può diventare un fattore competitivo

DI **EDOARDO SEGANTINI**

Non è un lavoro facile quello del Garante della Privacy, perché deve assicurare qualcosa che non sempre l'opinione pubblica adeguatamente apprezza e del cui valore si rende sempre conto. Tendiamo un po' tutti ad affrontare il problema distrattamente e sbrigativamente: le comodità dei servizi che troviamo su Internet ci inducono a prendere sottogamba i rischi per la sfera privata e gli accorgimenti per evitarli. Talvolta anche a causa della farraginosità delle stesse procedure di garanzia.

È questo uno degli argomenti che Antonello Soro, responsabile dell'Authority per la protezione dei dati personali, affronterà nella sua Relazione annuale del 28 giugno. Di cose da dire ne avrà parecchie, perché l'ultimo anno ha portato alcune grosse novità di scenario cui hanno contribuito, in modo significativo, l'esperienza e gli orientamenti normativi maturati nel nostro Paese.

«La prima novità — dice Soro — è l'approvazione, dopo quattro anni, del Regolamento europeo in materia di protezione dei dati personali, uno strumento importante per tre ragioni. In primo luogo perché armonizza la materia nei ventotto Paesi dell'Unione. Poi perché adegua le regole all'evoluzione tecnologica, per esempio alla crescita dei social network e dei big data. Infine perché istituisce la figura del privacy officer aziendale, il responsabile dei dati».

Il regolatore europeo, dice il magistrato, sta cambiando approccio verso le aziende che usano le informazioni sui clienti a scopo di marketing: si scommette sul fatto che, per le imprese, una politica corretta e ben comunicata della privacy sia un importante vantaggio competitivo nei confronti dei concorrenti: un'attività conveniente. Di conseguenza si introducono poche regole chiare e si prevede di intervenire con le sanzioni a posteriori, nel caso in cui le norme non siano rispettate. Il cambiamento del resto è già in corso. E non a caso è più veloce nei settori dell'economia, come assicurazioni e banche, dove trasparenza e cura nella gestione dei dati e della privacy possono essere l'elemento che fa la differenza nella scelta del cliente.

«L'altra grossa novità di quest'ultimo anno — dice Soro — è nel rapporto tra le authority e gli Over the Top, le multinazionali della Rete come Google, Facebook e Amazon. Lo scandalo Datagate, con le rivelazioni di Edward Snowden sulle schedature di cittadini (anche europei) da parte della National Security Agency americana, ha cambiato l'atteggiamento degli stessi monopolisti della Rete, che oggi sono più attenti al problema. E temono un inasprirsi delle regole ma anche una crescita della vigilanza dell'utente sui dati che gli appartengono». Va infatti facendosi strada l'idea che i dati personali, così come accadde a fine anni 90 con le reti di telecomunicazione, siano una risorsa da togliere ai monopoli e da liberalizzare. Oggi ad esempio, se un utente vuole, può uscire da Facebook, ma i suoi dati personali (su usi, gusti e preferenze) restano proprietà del monopolio social.

«A partire dal maggio 2018 — dice Soro — entrerà in vigore la portabilità dei dati personali: che, come il numero telefonico o il mutuo per la casa, potranno essere spostati da un'azienda all'altra». E diventare, aggiungiamo noi, oggetto di un negoziato in cui l'utente potrà cercare la controparte che gli offre le condizioni migliori. È probabile che, sulla spinta della convenienza, cresca anche la sensibilità dell'opinione pubblica al tema e si riduca il numero degli "indifferenti».

Tra le authority europee quella italiana è stata forse la prima a cercare la strada dell'accordo con Google. Con quali risultati? «Le garanzie che chiedevamo sono state introdotte, soprattutto in termini di consenso dell'utente. Siamo invece meno soddisfatti del modo in cui i dati delle persone continuano ad essere raccolti a loro insaputa, incrociando i servizi offerti: dall'email al motore di ricerca. Si è comunque fatto un doppio passo avanti nell'ottenere il riconoscimento dell'autorità nazionale e nell'affermare il rispetto di alcune regole».

Un primo passo — novità degli ultimi giorni — è stato compiuto anche con Facebook. Dopo averlo chiesto inutilmente al social network, un utente si è rivolto al Garante per ottenere la rimozione di foto compromettenti mediante le quali veniva ricattato da una donna con cui aveva intrattenuto una relazione. «Noi ci siamo mossi: e Facebook ha assicurato che provvederà entro dieci giorni. In sostanza vogliamo introdurre anche nel mondo virtuale le regole che valgono in quello reale».

Nella sua Relazione il presidente parlerà anche di «diritto all'oblio», la possibilità di vedere cancellate dal web notizie di fatti conclusi da tempo e non rilevanti ai fini della cronaca e della storia. E' infatti al Garante che si rivolgono le persone che vogliono presentare richieste di questo tipo. Spesso vengono accolte, ma non sempre.

Recentemente, ad esempio, tra i richiedenti c'è stato un ex terrorista. In quel caso il «diritto all'oblio» è stato negato con la motivazione che i fatti in questione rappresentano, purtroppo, un pezzo di storia che non può e non dev'essere rimosso.

@SegantiniE


UnipolSai Piano hi tech E adesso Cimbri monta la scatola (nera)

La privacy? Può diventare un fattore competitivo

Il Messaggero

Data 22-06-2016
Pagina 11
Foglio 1

Niente oblio sul web per l'ex terrorista

IL CASO

ROMA Niente diritto all'oblio su Google per gli ex terroristi: gli anni di piombo non si cancellano. Il Garante per la privacy respinge il ricorso di un ex protagonista «di una delle pagine più buie della storia italiana» che, finita di scontare la sua pena nel 2009, aveva chiesto a Google di deindicizzare alcune pagine relative al suo passato. Nonostante il tempo trascorso, spiega il Garante, «non può che prevalere il rispetto della memoria collettiva e il diritto dell'opinione pubblica a conoscere».

LA RICHIESTA

Secondo l'agenzia Ansa si tratterebbe di Roberto Nistri, romano, classe '58, ex Nar, condannato all'ergastolo per omicidi, uscito dal carcere per liberazione anticipata nel 2000 dopo 18 anni, biologo marino, fotografo professionista specializzato in natura e animali. L'ex terrorista si era rivolto a Google per chiedere di cancellare alcuni indirizzi e suggerimenti di ricerca visualizzati automaticamente. Incassato il no di Google, si è rivolto al Garante, sostenendo di essere un libero cittadino, danneggiato gravemente dalla presenza in rete di contenuti così datati nel tempo e «fuorvianti rispetto all'attuale percorso di vita».

In ballo c'è il diritto all'oblio, stabilito da una sentenza della Corte di Giustizia Ue del 2014, che contempla appunto la cancellazione dai motori di ricerca di link riferiti a notizie ritenute «inadeguate o non più pertinenti». Una questione diventata centrale, tanto più perché «la memoria permanente della rete ci pone di fronte a problemi nuovi e complessi e a scelte difficili», come riconosce lo stesso Antonello Soro, presidente dell'Autorità per la protezione dei dati personali.

«Per questo sul diritto all'oblio, dentro il perimetro dei criteri fissati in ambito europeo, ogni singolo caso merita una valutazione specifica», sottolinea. In questa circostanza è stato usato «un criterio di valore, di effettiva attualità dell'informazione e di reale interesse pubblico. Un conto è la richiesta di una persona che abbia commesso un reato, ma la cui vicenda non ha avuto rilievo per la storia del Paese. Altro conto è chi si macchia di delitti che sono ancora vivi nella storia dell'Italia e che hanno segnato pagine drammatiche per la comunità nazionale».

R.I.


Maturità al via, ed è guerra al mercato nero delle tracce

Niente oblio sul web per l'ex terrorista

CORRIERE DELLA SERA

Data 22-06-2016
Pagina 35
Foglio 1

SE IL DIRITTO ALL'OBLIO NON CANCELLA LA STORIA

Il terrorismo non si cancella. Il Garante della Privacy ha bocciato il ricorso di un ex terrorista italiano sulla rimozione da parte di Google dei contenuti che riguardano il suo passato. Oggetto di discussione, il diritto all'oblio.

Risvolto della questione, la lotta tra il diritto alla privacy e il diritto all'informazione. Già nel leggere le prime righe del provvedimento pubblicato ieri nella newsletter del Garante ci si scontra con la complessità del tema. «XY ha finito di scontare la pena nel 2009 per gravi di fatti di cronaca di cui è stato protagonista tra la fine degli anni 70 e i primi anni 80», recita il testo.

Si parla degli Anni di Piombo, di vicende che ci hanno segnato. Il Garante ha deciso di difendere la storia. Eppure non può divulgare il nome del protagonista. Secondo passaggio: XY ha chiesto la rimozione da Google di articoli e di suggerimenti di ricerca che lo associano alla parola terrorista. Ma sia Big G che il Garante gli hanno risposto picche. «Le informazioni di cui si chiede la "deindicizzazione" fanno riferimento a reati particolarmente gravi», recitano le motivazioni.

Non importa dunque che dagli Anni di Piombo a oggi sia passato molto tempo. E non importa nemmeno che nel 2013 la Corte di Cassazione abbia dato ragione a un ex Prima linea che faceva una richiesta del tutto simile. Dal maggio 2014 alle richieste «tradizionali» si sono aggiunte quelle che riguardano Internet. Google, adeguandosi a una sentenza della Corte di giustizia dell'Unione Europea, consente l'esercizio del diritto all'oblio anche in Rete. Da allora 33.633 sono le richieste arrivate solo dall'Italia.

E se nel 32,2 per cento dei casi Google le ha soddisfatte, in questo ultimo frangente ha deciso di rifiutare, supportato dal Garante. Però non è sempre andata così. Quando si aprì il contenzioso su Renato Vallanzasca, venne fuori che Wikipedia rischiava di dover far sparire centinaia di voci. Allora Jimmy Wales, cofondatore dell'enciclopedia digitale, tuonò: «La storia è un diritto umano. Nascondere la verità è profondamente immorale». Parole che viene difficile non condividere, soprattutto se si parla di terrorismo. Ma che nell'era di Internet hanno implicazioni da non sottovalutare.

Marta Serafini

Il Sole 24 ORE

Data 29-06-2016
Pagina 43
Foglio 1

Privacy. La relazione del Garante Antonello Soro al Parlamento

Per bilanciare privacy e diritti vale il principio di proporzionalità

Antonello Cherchi
ROMA

La tecnologia insidia la **privacy**. Non bisogna lasciarsi ammaliare dalle lusinghe delle potenzialità del **web**, che rende la vita più semplice grazie ai nuovi servizi, ma spesso a prezzo della perdita della nostra identità. I dati personali hanno infatti un grande valore economico, come dimostra la crescita del crimine informatico, che a livello mondiale ha raggiunto i 500 miliardi l'anno - poco dietro il narcotraffico - e in Italia nel 2015 è aumentato del 30 per cento.

Il monito arriva dal Garante della privacy, Antonello Soro, che ieri ha presentato al Senato, alla presenza del presidente di Palazzo Madama Pietro Grasso, la relazione sull'attività svolta dall'Authority nel 2015.

È «indispensabile - ha sottolineato Soro - promuovere una maggiore consapevolezza sulle intrinseche ambivalenti potenzialità che ogni tecnologia può comportare», in modo da «contrastare l'idea che sia inesorabile una progressiva riduzione degli spazi di libertà e intimità individuale».

La posta in gioco è alta e coinvolge la nostra riservatezza e con essa la nostra autonomia: «si pone un problema di libertà - ha affermato il Garante - se nell'economia fondata sui dati» non siamo capaci di proteggerli. Complice anche il fatto che il potere di profilazione è in mano a poche aziende, e questo «condiziona sempre più il mercato mondiale dei consumi e, più in generale, orienta le scelte personali».

Un argine è il modello europeo di tutela della privacy, modello che rappresenta, secondo Soro, un'«autentica bussola nel pianeta connesso» e può diventare «lo strumento attraverso il quale le nostre imprese possono competere con i giganti del web e trovare un ruolo non subalterno nella geografia dell'economia mondiale».

Per evitare uno sbilanciamento dei diritti bisogna sempre di più fare riferimento al principio di proporzionalità. Lo si deve fare nel campo del lavoro, dove la riforma del Jobs Act ha imposto nuove regole in materia di controllo a distanza; in quello della trasparenza pubblica, che ha ampliato il diritto di accesso dei cittadini agli atti della Pa; nella digitalizzazione della sanità; nella giustizia, che nelle indagini tradizionali utilizza strumenti pervasivi come i software-spia; nella lotta al terrorismo, dove non è la massiccia raccolta di dati ad aiutare le attività di intelligence, ma la loro interpretazione. Come ha ricordato Grasso, «spiare tutti non è possibile e non serve a niente».


«Più sinergie sulle politiche attive»
Bilancine privacy e diritti sul principio di proporzionalità
EXECUTIVE BUSINESS EDUCATION
COSTRUISCI LA TUA CARRIERA NEL MERCATO GLOBALE

Il Messaggero

Data 29-06-2016
Pagina 14
Foglio 1

Il Garante della privacy: «Allarme Cybercrime»

LA RELAZIONE

ROMA I crimini informatici, in Italia, nel 2015, sono aumentati del 30%, con una crescita del 50% di phishing e del 135% di ransomware. È un vero allarme quello lanciato ieri da Antonello Soro, presidente Autorità Garante per la protezione dei dati personali, alla presentazione della Relazione annuale 2015 in Senato. «Il peso attuale del cybercrime sull'economia mondiale - afferma Soro - viene stimato in 500 miliardi di euro all'anno, di poco al di sotto del narcotraffico nella classifica dei guadagni illeciti». Nell'ultimo anno sono state 49 le comunicazioni di data breach - quasi il doppio dell'anno precedente - nei servizi di comunicazione elettronica. Poco meno di 1700 - quasi triplicate - le violazioni amministrative contestate dal Garante. Circa tre milioni e 400mila euro le sanzioni amministrative riscosse.

Ancora, 25.560 le risposte a quesiti degli utenti. Circa 3.000 le segnalazioni per casi di telemarketing aggressivo, nei primi sei mesi del 2016. Per Soro, «L'Europa ha oggi la straordinaria opportunità di proporre, su scala mondiale, il proprio modello di protezione dei dati quale autentica bussola nel pianeta connesso, capace di coniugare al punto più alto i diritti delle persone con le esigenze del mercato». E può diventare «lo strumento attraverso il quale le nostre imprese possono competere con i giganti del web e trovare un ruolo non subalterno nella geografia dell'economia mondiale». L'Italia si candida a modello.

Valeria Arnaldi


Scuola, da settembre la pagella ai presidi con premi e punizioni

Avvenire

Data 29-06-2016
Pagina 13
Foglio 1

Privacy. I crimini informatici costano 500 miliardi l'anno

Maurizio Carucci
Roma

La tutela della riservatezza sul web e la gestione dei dati personali nelle politiche di sicurezza. Per il presidente del Senato Pietro Grasso – intervenuto ieri a Palazzo Madama alla presentazione della Relazione del Garante per la protezione dei dati personali – sarebbero queste le priorità. «Da una parte – ha spiegato Grasso – sono inutili e pericolose quelle forme di sorveglianza di massa che alcuni Paesi stanno adottando dopo gli attacchi terroristici in Europa. Spiare tutti non è possibile e non serve a niente: si devono invece potere controllare le persone che sono legittimamente destinatarie di indagini, in base a precise regole, di procedura e di sostanza. Al tempo stesso lo sforzo è costringere i gestori delle piattaforme web a consentire l'identificazione e il controllo di chi commette reati attraverso internet».
Con la diffusione del web e degli strumenti digitali, anche l'attività dell'Autorità garante della privacy è aumentata. Lo scorso anno sono stati quasi 5mila i quesiti, i reclami e le segnalazioni prese in esame, con specifico riferimento a settori quali il marketing telefonico; il credito al consumo; la videosorveglianza; il credito; le assicurazioni; Internet; il giornalismo; la sanità e i servizi di assistenza sociale. Poco meno di 700 i provvedimenti collegiali adottati. Quasi triplicato il numero delle violazioni amministrative contestate: nel 2015 sono state circa 1.700. Le sanzioni amministrative riscosse ammontano a circa 3,5 milioni di euro.
Sono alcuni dei dati contenuti nella Relazione annuale, illustrata dal presidente dell'Autorità Antonello Soro. Sono stati decisi 307 ricorsi, riguardanti soprattutto banche e società finanziarie; datori di lavoro pubblici e privati; attività di marketing; editori (anche televisivi); banche e società finanziarie; pubblica amministrazione e concessionari di pubblici servizi; società di informazioni commerciali; informazioni creditizie; marketing. Da segnalare anche 33 violazioni trasmesse all'autorità giudiziaria, in particolare per la mancata adozione di misure minime di sicurezza a protezione dei dati.

Nel 2015 incremento dei reati del 30% in Italia Grasso: tutela della riservatezza e gestione dei dati personali sono prioritari Soro: dimensioni inquietanti e difficoltà di protezione

La Relazione, inoltre, ha posto l'accento sulla minaccia costituita dal cybercrime, che pesa sull'economia mondiale ben 500 miliardi di euro l'anno, come il narcotraffico. E l'Italia lo scorso anno ha subito un incremento del 30% dei crimini informatici (+50% *phishing*, ossia l'invio di messaggi di posta elettronica che imitano, nell'aspetto e nel contenuto, messaggi legittimi di fornitori di servizi per rubare dati e codici di accesso; +135% *ransomware*, un sistema che limita l'accesso del dispositivo che infetta, richiedendo un riscatto da pagare per rimuovere la limitazione), particolarmente rilevanti nel settore delle imprese. «La criminalità informatica ha assunto dimensioni inquietanti – ha sottolineato Soro – sono oggetto di minacce credenziali e identità digitali di milioni di utenti e naturalmente la superficie di attacco cui siamo esposti aumenta in proporzione alla mole dei dati disseminati nel web», e con una velocità «maggiore della nostra capacità di proteggerla».
Il Garante italiano, primo tra quelli europei, ha dato prescrizioni a Google, ha consolidato nel 2015 la procedura di confronto e controllo del protocollo sottoscritto da Mountain View. A Facebook l'Autorità ha imposto di bloccare i falsi profili e di assicurare più trasparenza e controllo agli utenti. Per quanto riguarda la fiscalità e l'adozione del 730 precompilato, l'Authority è intervenuta per richiedere precise misure tecniche e organizzative per proteggere i dati dei contribuenti.

Il Messaggero

Data 19-07-2016
Pagina 22
Foglio 1

L'intervento

Antiterrorismo, l'arma in più della "Cyber security"

Paolo De Angelis

La crescente minaccia terroristica velocemente costringe i governi di tutto il pianeta ad aggiornare l'agenda alla voce sicurezza, per prevenire i rischi di attentati che, con drammatica cadenza, vengono realizzati in ogni latitudine. Non ci possono essere falle, la prevenzione è indispensabile di fronte ad un fenomeno sempre più violento e diffuso. Gli scenari mondiali sono in continuo aggiornamento per stabilire standard comuni di coordinamento antiterrorismo. In questo quadro, oltre agli interventi sul versante della sicurezza fisica dei cittadini, assume sempre maggior rilievo lo scenario informatico e la sicurezza dello spazio cibernetico. I maggiori analisti del mondo sono al lavoro per individuare i rischi che la rete informatica può correre in caso di attacco terroristico, per attuare strategie di prevenzione e risposta. C'è la consapevole certezza che un'azione terroristica informatica sia in grado di causare danni e conseguenze non meno devastanti di quelli tradizionali, per il rischio di completa paralisi di servizi e settori essenziali.
L'antiterrorismo non è più solo di tipo militare o di controllo del territorio ma di tipo informatico, contro i rischi della cyber war, lessico anglosassone che evoca scenari di crimini cibernetici di altissimo livello, in grado di mettere in ginocchio lo Stato aggredito, contro i quali la risposta deve essere efficace e pronta. L'Italia ha adottato il Piano strategico nazionale per la sicurezza cibernetica e la protezione informatica, un testo normativo della Presidenza del Consiglio dei Ministri che detta le linee guida di prevenzione e di reazione in caso di attacco ai sistemi informatici sia pubblici che privati; è la prima volta che la sicurezza del comparto industriale e produttivo viene messa sullo stesso piano di quella dei sistemi telematici militari o della pubblica amministrazione in genere. È un salto culturale nella strategia della sicurezza perché considera il problema non solo nei tradizionali ambiti istituzionali ma in ogni aspetto della rete economica, organizzativa e strutturale del sistema Paese. L'impostazione del quadro strategico nazionale della cyber security risente positivamente delle influenze e delle esperienze di altri paesi che ci hanno preceduto, a volte di anni, nella visione della sicurezza informatica come priorità nazionale. Una normativa con molte luci, prima fra tutte l'individuazione e la previsione di azioni di prevenzione e di contrasto; infatti, dal primo testo in materia dell'anno 2013, che ha disegnato l'assetto istituzionale della sicurezza cibernetica, si è passati, nel dicembre 2015, ad un testo molto più completo ed operativo, anche grazie al significativo stanziamento di 150 milioni di euro destinato a realizzare concretamente il piano. Ci sono però anche le ombre, specie nella ripartizione dei ruoli e nella gerarchia dei protagonisti della strategia di sicurezza informatica: l'eccesso di organismi coinvolti e la suddivisione delle competenze tra i diversi ministeri (ben 6) e centri di coordinamento tecnico (ulteriori 7 soggetti istituzionali oltre agli operatori privati che gestiscono reti telematiche) rischia di burocratizzare l'azione, a discapito dell'efficienza e della immediatezza della risposta in caso di attacco, anche se il piano assegna il ruolo centrale nella gestione del sistema di sicurezza alla Presidenza del Consiglio, con funzioni di vertice sul piano decisionale ed organizzativo; tutto il piano strategico ruota attorno alle informazioni che devono transitare da un soggetto ad un altro in tempo reale, per le immediate contromisure in caso di attacco informatico e più è lunga la catena di comando, più lungo è il percorso delle informazioni prima di giungere al livello delle azioni. Ma anche se il meccanismo avrà necessità di essere regolato per garantire la massima efficienza, è già positivo che ci sia una struttura in grado di operare in caso di rischi di sicurezza della rete informatica e telematica italiana; la filosofia di fondo è che le politiche di Cyber Strategy non siano solo una mera tecnica, per le sofisticate conoscenze che richiedono, quanto una vera e propria strategia, intesa come risposta globale ed articolata, in cui la sicurezza sia un valore assoluto da tutelare, anche in un contesto non tradizionale ed in continua evoluzione come il crimine informatico. La parola chiave è quindi cultura: della sicurezza dei dati, delle informazioni e, in generale, delle risorse di cui i soggetti, pubblici o privati, dispongono; poi, cultura della protezione del patrimonio di conoscenza dei singoli, privati o pubblici, e degli interessi superiori dello Stato; infine, cultura informatica, per lo sviluppo della consapevolezza che il mondo web oramai coincide col mondo reale e la violazione delle reti informatiche non ha solo dimensione virtuale ma ha riflessi significativi anche sui rapporti giuridici ed economici concreti. È il momento di agire, allora: il terrorismo non aspetta.

Sostituto procuratore presso il Tribunale di Cagliari

Il Sole 24 ORE DOMENICA

Data 07-08-2016
Pagina 19
Foglio 1

TRA DIRITTI E SICUREZZA

La libertà in tempi di terrorismo

di **Carlo Melzi d'Eril**
e **Giulio Enea Vigevani**

«In un tempo tremendo in ogni parte del mondo» anche pensatori di fede liberale si lasciano tentare dalla seguente suggestione: in una logica di guerra, occorre rinunciare ad alcuni diritti democratici, per arginare l'offensiva terrorista. Simile ragionamento viene declinato soprattutto con riguardo a talune libertà esercitate sulla rete Internet, da alcuni equiparata, invero sommariamente, a uno strumento di lotta e di combattimento. E, in effetti, l'ambiente telematico non è più solo un mezzo di diffusione di messaggi. La rete è divenuta un vero e proprio "luogo" di incontro, dove nascono o comunque si sviluppano anche associazioni terroristiche. Gli affiliati non hanno più bisogno di trovarsi *vis-à- vis*; ognuno di loro può rintracciare online il messaggio ispiratore dell'azione violenta e, sempre online, stringere quei legami nell'ambito dei quali pure nasce la pianificazione delle attività illecite.

La questione sembra coinvolgere soprattutto due libertà: quella di comunicare in modo riservato e quella di esprimersi. In relazione a questi due ambiti, la rete deve avere una disciplina sua propria, derogatoria dei principi generali? Proviamo a fare qualche esempio: sarebbe possibile consentire una verifica "a largo raggio" da parte delle forze dell'ordine della corrispondenza e-mail di alcuni soggetti solo perché appartenenti a una determinata religione? E comunque, ciò sarebbe auspicabile? Oppure, potrebbe essere organizzata una forma di controllo così capillare da realizzare una sorta di schedatura di tutti coloro che provengono da determinati Paesi, in base alle espressioni che utilizzano in rete, anche su piattaforme pubbliche come ad esempio i social network? Infine, sarebbe concepibile bloccare un sito Internet, imponendo magari ai provider di non diffonderne i contenuti nel territorio dello Stato, solo in base al fatto che contenga generiche espressioni di compiacimento per le azioni terroristiche?

I cosiddetti "doppi binari" – ovvero discipline differenti di un medesimo istituto, se calato in contesti diversi – nel nostro ordinamento sono più di uno e, in casi come la lotta alla criminalità organizzata, sotto più aspetti appaiono anche opportuni. Nel nostro quadro costituzionale, le discipline dettate dall'emergenza possono tuttavia incidere su alcuni piani e non su altri. Possono influenzare le modalità di esecuzione di atti di indagine, condizionandone tempi e modi (come i casi e la durata delle intercettazioni). Possono, altresì, determinare l'introduzione di reati, qualora ci si trovi di fronte a condotte nuove, che aggrediscano davvero interessi costituzionalmente tutelati (come forse è nel caso dei reati di addestramento, arruolamento e organizzazione di trasferimenti per finalità di terrorismo). Ciò che però non riteniamo né possibile né auspicabile è consentire, pure davanti a concrete e ben percepite emergenze, di incidere sui principi che tutelano le libertà civili, graduandone l'estensione e l'ampiezza di applicazione.

Un primo punto da chiarire è l'esistenza o meno di uno stato di guerra. Nonostante non pochi siano di contrario avviso e il termine abbia fatto capolino tra i titoli di alcuni giornali e addirittura nelle parole del Pontefice, continuiamo a pensare che, per quanto tragica sia la conta di morti e feriti dopo i numerosi attentati, non ci troviamo a combattere una guerra. Non almeno nel senso accolto dal nostro ordinamento costituzionale, ovvero un fatto di violenza collettiva potenzialmente in grado di rompere gli equilibri tipici di uno Stato, sovvertendone l'ordine, l'integrità non solo territoriale, e la sua medesima sopravvivenza. D'altronde, della guerra mancano i presupposti, manca la dichiarazione e mancano pure gli Stati ostili. Allora, se non si tratta di una guerra, il fenomeno del terrorismo nella sua odierna manifestazione, come è accaduto in passato nel nostro Paese, non può giustificare una "risposta bellica", una sospensione delle libertà fondamentali proprie dello stato di guerra.

Come lucidamente sostiene un magistrato torinese esperto di questa materia, Alberto Perduca, la risposta più credibile e nel lungo periodo più efficace contro il terrorismo islamico è quella del diritto penale - capace di mantenere un equilibrio tra tutela dell'individuo e sicurezza - oltre che della cooperazione internazionale e dell'attività di intelligence. E così anche per il tema della libertà di espressione nella rete si possono prospettare risposte efficaci all'interno del recinto dello stato di diritto. Sotto quest'ultimo profilo, va sottolineato che il nostro sistema in linea di principio non esclude a priori dal dibattito pubblico chi rifiuti le idee di libertà e democrazia. La nostra democrazia, cioè, non è una "democrazia protetta", che tende quindi a espellere le convinzioni contrastanti con i propri principi. Dunque anche l'opinione sgradevole e finanche molesta trova cittadinanza sino a che non diventa istigazione a delinquere o gratuitamente offensiva. Per di più, in questo caso, forse, non è sbagliato richiamare la portata del principio di uguaglianza, di cui all'art. 3 della Carta che, lungi dall'essere una norma per così dire "buonista", si pone come argine insuperabile a qualunque discriminazione basata su «sesso, razza, lingua, religione, opinioni politiche, condizioni personali e sociali». E, si badi, le ragioni ideali, quando non prendono spunto da matrici fideistiche, laiche o religiose, hanno sempre un fondamento di grande concretezza: graduare oggi la libertà per una ragione qualsiasi consente, domani, di farlo per una ragione diversa, magari non altrettanto nobile.

Insomma, lo Stato di diritto, se non è in gioco la sua sopravvivenza, si comporta come tale anche di fronte a chi gli si dichiara ostile. Quale è dunque il limite entro cui l'intervento sulla libertà di espressione è accettabile? Nel nostro sistema tale diritto è tutelato al massimo solo se lo si esercita alla luce del sole («tutti hanno il diritto di manifestare il proprio pensiero») e non a caso è punito chi pubblichi uno stampato senza il nome dell'editore. In altri termini, nell'area incomprimibile di protezione offerta dall'art. 21 Cost. non sembrano rientrare le opinioni anonime. Ciò corrisponde a quel *fil rouge* del nostro ordinamento per il quale alla massima libertà deve corrispondere la massima trasparenza: nella democrazia, quale noi vogliamo fermamente continuare a essere, non si deve avere timore di esprimersi a viso aperto. In quest'ottica, sarebbe forse ipotizzabile l'oscuramento anche preventivo di un sito internet se non rende chiara l'identità dei soggetti responsabili, qualunque sia il contenuto. Potrebbero altresì essere introdotte regole per imporre ai siti di identificare i soggetti che vi pubblichino notizie o commenti. Infine, sarebbe immaginabile la conservazione di dati tratti dall'accesso al web per un tempo maggiore per i soggetti che tentino di nascondere la loro identità. In conclusione, ci piace ribadire che l'attenzione nel tracciare i confini entro i quali il legislatore può agire non è frutto di un puntiglio né di ingenuità o di scarso attaccamento ai valori che contraddistinguono il nostro Stato, di matrice occidentale, liberale, democratico. È invece tutto il contrario: come scrive un acuto penalista, Francesco Viganò, bisogna trovare il modo di difendersi senza «con ciò sacrificare il patrimonio di diritti umani che costituisce in fondo il più autentico motivo di orgoglio delle nostre società».

QN
IL GIORNO il Resto del Carlino LA NAZIONE

Data 09-09-2016
Pagina 31
Foglio 1

Viaggio nel lato oscuro della Rete «Il deep web non va demonizzato»

Il semiologo Fabbri: «La trasparenza assoluta induce al totalitarismo»

Parola di esperto

Gli abissi di Internet non sono abitati solo dal crimine: servono a chi lotta contro le dittature

di LORENZO GUADAGNUCCI

LA RETE è un iceberg e quel che vediamo abitualmente, il world wide web, non è che la punta affiorante dall'acqua, appena il 4% del totale. Tutto il resto è «comunicazione al nero», come l'ha chiamata il semiologo Paolo Fabbri nella sua conferenza al Festival della Comunicazione di Camogli.

Professor Fabbri, che cos'è la comunicazione al nero?

«Le cito i dati di una ricerca: ogni giorno su Facebook passano 350 milioni di foto e circolano 144 miliardi di mail. Un'enormità, ma - appunto - la comunicazione in chiaro non è che il 4% del totale. Abbiamo un'idea della comunicazione - chiara, trasparente, aperta - che non corrisponde alla realtà. Possiamo dividere la comunicazioen al nero in due ambiti: il "dark web", dove la comunicazione è criptata, ma è sempre qualcosa di conoscibile e conosciuto, accessibile con strumenti come il software Tor. Poi c'è il "deep web"».

COMUNICARE IN NERO
«Anche il segreto fa parte della nostra vita: anzi, ha un suo valore sociale»

È pericoloso?

«Il deep web è un enorme mercato, dove si trovano droga, armi, pedofilia, commercio di organi e dove si usa una moneta virtuale che permette di non lasciare tracce. D'altra parte è anche il luogo che permette ai militanti che si oppongono alle dittature di comunicare e organizzarsi: accade in Cina, è successo con le primavere arabe».

Quindi, pro o contro il deep web?

«È la domanda che dobbiamo farci sulla scia del quesito che Umberto Eco ha lanciato riferendosi al web in chiaro, che una volta definì popolato di imbecilli. La mia risposta sul deep web è: pro e contro, contro e pro. Il mio è un giudizio reversibile. La trasparenza va benissimo, ma non sempre».

Oggi la trasparenza in Rete è invocata anche per la lotta al terrorismo.

«Appunto, ma io dico che la domanda sul deep web pone un falso quesito, perché si sofferma sulla tecnica e trascura la tecnologia. Io faccio una precisa distinzione: la tecnologia è l'uso sociale che si fa della tecnica, è può quindi essere criminale ma anche l'opposto, cioè socialmente utile».

Quindi è sbagliato demonizzare il deep web?

«È sbagliato, ma certo non dico che non si debbano perseguire le attività criminali, tutt'altro. In un certo senso il deep web è utile anche alla polizia, che lì può riuscire a scoprire e inseguire chi compie dei crimini. C'è una tensione continua fra trasparenza e privacy. Quando il governo statunitense ha chiesto alla Apple di aprire la sua criptografia per gli smartphone, la risposta è stata no».

Ma non c'è il pericolo di agevolare terroristi e criminali?

«Guardi, le ultime indagini hanno rivelato che i membri dell'Isis usano poco il deep web, che è difficile utilizzare, e preferiscono il web in chiaro, dove comunque è possibile agire con forme di protezione e riservatezza. La società dell'informazione nella quale viviamo è anche la società della massima diffusione della criptografia e dello spionaggio. Non c'è mai stato tanto spionaggio come oggi. Il dilemma è evidente: eliminando la criptografia si renderebbe forse la vita più difficile ai terroristi, ma ci sarebbe un prezzo molto alto da pagare in termini di libertà. Il ministro degli Interni francese in effetti è stato chiaro: è contro la criptografia in nome dell'emergenza, cioè di una guerra, ma in guerra c'è il controllo dell'informazione».

Dobbiamo dunque convivere con l'informazione al nero?

«Io credo che dobbiamo riconoscere il ruolo costitutivo del segreto. Segreto non come mistero, sia chiaro, ma come non detto. C'è stato un periodo in cui la psicanalisi diceva che il paziente deve dire tutto, non nascondere niente. Poi si è capito che c'erano più difficoltà e pericoli di quanto si immaginasse e anche lo psicanalista ammette che qualcosa possa rimanere segreto. Il non detto fa parte della nostra vita, del modo di essere di ciascuno. A livello sociale vale lo stesso principio. Pensi alla politica. La comunicazione politica è fatta di polemica e non c'è polemica senza una parte di segreto, di non detto. Non c'è politica senza allusività. C'è ancora chi ritiene che la tecnologia della comunicazione, di per sé, porti democrazia, ma non è così. Chi lo pensa ritiene che chi parla dica tutto, con chiarezza e trasparenza, ignorando l'importanza del non detto e dell'allusività. Potremmo anzi ribaltare il concetto e dire che in un mondo in cui tutto è visibile incombe il totalitarismo. Il sogno del dittatore è la trasparenza totale».

La trasparenza è oppressiva?

«Ci può essere un'oppressione della trasparenza, come può esserci, è chiaro, un'oppressione del segreto. Ma c'è un'ideologia della trasparenza che non considera quanto questa possa essere alienante».

CORRIERE DELLA SERA

Data 14-09-2016
Pagina 24
Foglio 1

La sfida agli hacker dei voli

L'INCHIESTA SICUREZZA HI-TECH

I software in vendita via web per pochi euro riescono a elaborare 300 milioni di password Le contromosse di compagnie aeree e Fbi

Cinque minuti per accedere al sistema di comunicazione tra aereo e torre di controllo. Due giorni per modificare — dalla terraferma — i parametri del «Flight Management System», l'interfaccia di gestione di un volo. Quando Patrick Ky, direttore dell'Agenzia europea della sicurezza aerea (Easa), ha visto i risultati del pilota-hacker che aveva ingaggiato per testare le vulnerabilità, non ha avuto dubbi: bisogna attivare il prima possibile una squadra di pronto intervento, 50-60 poliziotti digitali, che in ogni momento possano fermare un attacco informatico ai velivoli e agli aeroporti. «Perché l'unica certezza è che comunque qualcuno ti aggredirà», ragiona Kurt Pipal, agente dell'Fbi ed esperto informatico.

Negli ultimi due anni sono in netto aumento gli attacchi cibernetici nel settore dell'aviazione. I jet sono sempre più connessi. Almeno 52 compagnie nell'intero pianeta — calcola la società Routehappy — offrono il wi-fi a bordo in quasi tutti i loro voli. Un numero maggiore fornisce agli assistenti di bordo i tablet per gestire ogni fase del collegamento. Soltanto British Airways, per esempio, ha sviluppato una quarantina di applicazioni e consegnato a comandanti, hostess e steward 17 mila iPad.

Il tutto mentre su eBay è possibile acquistare per una manciata di euro software in grado di elaborare 300 milioni di diverse chiavi di accesso in pochi minuti fino a trovare la password effettiva. Poco più di un anno fa l'esperto di cybersicurezza Chris Roberts è stato fermato e interrogato dall'Fbi dopo aver scritto su Twitter che era in grado di accedere ai comandi di un aeromobile. Ai federali Roberts ha raccontato di essere riuscito a dare persino potenza ai motori di un jet.

Gli aerei sono diventati facili prede degli hacker? «La maggior parte dei velivoli che vola oggi e che offre servizio wi-fi non è stato costruito all'inizio per supportare, nella massima sicurezza possibile, la connettività», sostiene il maggior generale Linda R. Urrutia-Varhall, da poco direttore delle operazioni al National Geospatial-Intelligence Agency, l'ente che ha pedinato via satellite il nascondiglio pakistano di Osama bin Laden. «Il settore è al centro degli interessi dei terroristi e dei criminali, bisogna condividere di più le informazioni».

«Però nessun velivolo, ad oggi, è stato davvero hackerato nelle sue parti essenziali», dice al *Corriere* Pascal Andrei, vicepresidente di Airbus Group, da quindici anni il responsabile della sicurezza dei velivoli A380 e A350. Andrei è a capo di tutto quello che si muove dentro il colosso europeo in materia di protezione dagli attacchi informatici dei velivoli (civili e militari) e dei satelliti. «I nuovi aerei sono sempre più informatizzati e sempre più connessi, ma sono stati anche progettati di conseguenza — aggiunge —. Nell'A380 ci siamo basati sulla partizione: ogni blocco è separato dall'altro, a partire da quello dell'avionica (il vero computer di bordo, *ndr*)». E se i malintenzionati colpiscono i satelliti mandando in tilt il Gps? «L'aereo è dotato di un suo sistema di geoposizionamento».

Insomma, i sistemi «critici» per Andrei non sono attaccabili grazie anche alle leggi internazionali. «Quello che non è regolato è l'intrattenimento di bordo (chiamato Ife, *ndr*): qui la sicurezza è a carico del singolo vettore». «Gli hacker sono davvero entrati nell'Ife», conferma Alan Pellegrini, amministratore delegato di Thales Usa, azienda che produce strumenti aerospaziali. Una volta dentro, i malintenzionati possono rubare i dati delle carte di credito, intrufolarsi nelle caselle email, mandare virus per bloccare la visione dei film o rubarli».

«Finora abbiamo stabilito 29 scenari di rischio informatico», rivela Calin Rovinescu, ad di Air Canada. Scenari condivisi con le compagnie appartenenti a Star Alliance (la più grande alleanza del mondo) «che ha 18 gruppi che si occupano di cybersicurezza». «Bisogna usare di più gli hacker "buoni" per colmare le lacune informatiche», suggerisce Anja Kaspersen, capo dell'International Security del World Economic Forum. Cosa che in Airbus, chiarisce Pascal Andrei, fanno già: «Dal 2004 ne abbiamo 14 e si muovono sotto la nostra supervisione oppure si tengono aggiornati». Non saranno gli unici. «Molti altri, quando mi incrociano, chiedono di venire a lavorare in Airbus. E noi i migliori li prendiamo».

Leonard Berberi
lberberi@corriere.it

Il Messaggero

Data 15-09-2016
Pagina 1
Foglio 1 / 2

Giungla on line

Esistono norme ma senza tutele per la rimozione

Cristiana Mangani

Lasciate ogni speranza o voi che finite sul web, perché difficilmente riuscirete a far dimenticare il vostro nome o le vostre gesta. Non bastano, infatti, le regole attuali.

A pag. 3

Lo scandalo della gogna in rete il diritto all'oblio è senza tutele

▶Troppi punti deboli nelle regole: mancano strumenti per garantire la rimozione dei file

▶Il ruolo dei motori di ricerca: e anche se accettano di cancellare non basta

LA TUTELA

ROMA Lasciate ogni speranza o voi che finite sul web, perché difficilmente riuscirete a far dimenticare il vostro nome o le vostre gesta. Non bastano, infatti, le regole indicate da una sentenza della Corte di giustizia europea del 13 maggio del 2014, secondo la quale, tecnicamente, "sparire" dal mondo virtuale è possibile. Vedere riconosciuto "il diritto all'oblio" è cosa ben diversa, anche perché il primo stop è proprio nella difficoltà di stabilire fino a quanti anni di distanza dai fatti possa essere esercitato il diritto dell'individuo a ottenere la cancellazione dei propri dati. Ed è così che si spiega come mai, delle tantissime richieste di rimozione inviate dall'Italia, Google ne abbia accolte poco più del 30 per cento.

IL PRECEDENTE

La sentenza della Corte di giustizia ha garantito agli utenti il diritto a vedere cancellati sui motori di ricerca i link riferiti a informazioni personali ritenute «inadeguate o non più rilevanti». E ha trovato spunto da una vicenda che ha coinvolto Google in Spagna: nel 2009 un avvocato si è accorto che cercando il suo nome, veniva fuori una nota legale del 1998 pubblicata sul sito del quotidiano La Vanguardia che elencava i suoi debiti dell'epoca. Il giornale si era rifiutato di rimuovere le informazioni e altrettanto aveva fatto Google. L'avvocato, allora, aveva seguito tutto l'iter giudiziario fino ad arrivare davanti alla Corte europea, che aveva riconosciuto il suo diritto, fermo restando che andava verificato se ci fosse un interesse pubblico o un diritto alla privacy.

Ma come si esercita il diritto all'oblio, o più correttamente alla deindicizzazione? I colossi del web hanno aperto alla possibilità di essere cancellati proprio in seguito al verdetto del 2014. Google ha messo online una pagina per avanzare le richieste e, fino a luglio, i link cancellati ammontavano globalmente a 580 mila. L'Italia fino a quella data ha presentato 897 istanze legali, in calo rispetto alle 956 del primo semestre. La procedura è semplice: si inseriscono i propri dati, la url che si desidera venga eliminata e una copia del proprio documento d'identità. Se il processo va a buon fine, Google integra nei suoi algoritmi la richiesta e alla successiva ricerca fatta sul nome dell'utente quel link non apparirà più. Tuttavia, anche se il motore di ricerca decidesse di accogliere la richiesta di cancellazione, il vero nemico dell'oblio rimane la viralità, la diffusione sui social network, la possibilità che il contenuto, il video o le foto possano aver raggiunto server incontrollabili, magari con sedi in stati africani o in chissà quale parte del mondo. La url, quindi, se anche non dovesse più comparire quando qualcuno digiterà il nome dell'utente, potrebbe essere ancora raggiungibile tramite altre parole chiave.

LE SOLUZIONI

E non è tutto, perché Google potrà anche decidere di considerare la richiesta illegittima e negare la cancellazione del contenuto. A quel punto che fare? L'utente che deciderà di continuare la sua battaglia potrà fare ricorso al Garante per la privacy con una spesa di 150 euro e un'attesa di massimo 60 giorni. All'Authority spetterà il compito di accettare o respingere la procedura in base al bilanciamento con il diritto di cronaca: se un fatto è troppo recente o è di rilevante interesse pubblico, la risposta sarà negativa. E allora rimarrà solo la carta del giudice civile, e quindi il ricorso al diritto alla vita privata e alla riservatezza che, in qualche modo, coinciderà con il diritto all'oblio. Ma è

una procedura che comporterà un impegno economico maggiore a tempi decisamente più lunghi.
È più facile, comunque, ottenere la cancellazione di informazioni riguardanti dati personali piuttosto che notizie legate a fatti di cronaca, vicende giudiziarie o riprese dai mezzi d'informazione. In tanti vi hanno fatto appello non ottenendo soddisfazione. E' successo a Eva Mikula finita nell'inchiesta della Uno Bianca che chiedeva di vedere cancellato uno sceneggiato sui fratelli Savi dove veniva ritirata in ballo la sua vicenda, ma anche tutte le indicazioni che la riguardavano presenti sul web. Il giudice le ha dato torto. E altrettanto è successo a qualcuno vicino a Renato Vallanzasca che ha provato a far sparire le notizie on line sugli anni bui della banda.

Cristiana Mangani

IL TERMINE

Diritto all'oblio

Con la locuzione "diritto all'oblio" si intende una particolare forma di garanzia che prevede la non diffondibilità di precedenti pregiudizievoli dell'onore di una persona. In particolare, si fa riferimento a casi giudiziari che risalgano a molto tempo prima.

C'È UNA PROCEDURA PER FARSI DIMENTICARE MA LE INFORMAZIONI DA RIMUOVERE RESTANO SEMPRE RINTRACCIABILI CON ALTRE CHIAVI

Domande & risposte

A cura di Andrea Andrei

Si può eliminare un contenuto dal web? Come?

Sì. Nel caso di materiale lesivo per la privacy, come un filmato sessualmente esplicito, di solito basta utilizzare i servizi di segnalazione della piattaforma (la "bandierina" sotto i video di YouTube). Si può anche inviare una lettera al sito in cui si richiede la cancellazione del contenuto entro dei termini stabiliti. Se non si ottiene risposta, ci si può rivolgere al Garante della privacy o a un giudice. Per quanto riguarda i motori di ricerca, si può richiedere che link o pagine vengano deindicizzati. Google può far sì che certi risultati non appaiano.

Quanto tempo ci vuole per la rimozione?

Per tutti quei contenuti che violano la privacy, nel caso in cui la violazione è talmente evidente da non lasciare alcun dubbio di sorta (come ad esempio un filmato sessualmente esplicito) e la cui rimozione è perciò più urgente, spesso bastano pochi giorni o anche poche ore. Invece, per tutto quel materiale, attraverso cui si commettono altri tipi di violazioni (come ad esempio la diffamazione), i tempi sono normalmente più lunghi, perché la piattaforma ha un margine di discrezionalità per ciò che concerne l'applicazione del diritto all'oblio.

Come possono essere protetti i più giovani?

Con la consapevolezza. Alcuni consigli sono anche raccolti nel "Centro sicurezza" di Google, piattaforma dedicata all'educazione all'utilizzo del Web. Ad esempio, bisogna evitare a prescindere, di registrare filmati o scattare foto dal contenuto violento o sessualmente esplicito. Poi, il principio che vale è la cosiddetta "regola della nonna". Cioè, prima di condividere o pubblicare un contenuto, bisogna sempre chiedersi: «Lo mostrerei a mia nonna o al mio capo?». Mai pubblicare qualcosa solo perché qualcuno ce lo ha chiesto, specialmente se quel qualcuno è uno sconosciuto.

Come si può bloccare materiale hot?

Se si cancella subito il contenuto originale, appena pubblicato, forse sì. Ma se quel materiale viene preso da qualcun altro, salvato e ripubblicato su diverse piattaforme, bloccarne la diffusione diventa molto difficile, se non impossibile. Ad esempio poi, nel caso di YouTube, è necessario a quel punto richiedere la rimozione di ogni singolo video, e non c'è modo di eliminare tutti i filmati riguardanti un determinato argomento o una determinata persona. Ecco perché alcuni video che citano direttamente o indirettamente Tiziana Cantone sono ancora facilmente reperibili.

Esistono social network più sicuri?

È bene fare una premessa: condividere in Rete materiale sensibile, anche in una comunicazione tra privati, è sempre rischioso. Anche perché, se ci si fida di chi lo riceve, ciò non mette al riparo dall'eventualità che quel materiale possa essere sottratto da qualcun altro. Detto questo, i social network e le chat più conosciute sono generalmente affidabili e collaborativi. Servizi come Skype e altri come Snapchat non implicano il salvataggio di un contenuto ma solo la fruizione, possono essere meno rischiosi.

LA STAMPA

Data 15-09-2016
Pagina 3
Foglio 1

Come ci si può difendere

Per cautelarsi da immagini imbarazzanti gli strumenti giuridici sono inefficaci Così sul Web spopolano ricatti e gogne

I giuristi

L'avvocato che aiuta le vittime "Si possono limitare i danni però non eliminarli del tutto"

TORINO

L'avvocato Francesco Micozzi, che fa parte del Circolo dei Giuristi Telematici e che tratta casi come quello di Tiziana Cantone, ha una formula che ripete a tutti i suoi clienti: danno digitale permanente. Perché gli strumenti giuridici per intervenire quando sono lesi i diritti sulla rete esistono, ma al massimo si possono limitare i danni, non eliminarli del tutto. «I siti Internet sono infiniti e se è vero che i canali più diffusi hanno ormai policy avanzate, che permettono la cancellazione di dati e immagini in tempi rapidi, non si saprà mai se si sono eliminati tutti i contenuti, se questi ricompariranno su qualche altro sito minore, magari basato in uno Stato straniero e se si riuscirà anche solo a risalire al proprietario».

Per questo, più che di tutela piena, si parla di limitare i danni. Gli strumenti giuridici ci sono, ma non sono scudi impenetrabili. È possibile rivolgersi al tribunale civile per far valere il proprio diritto all'oblio, ma in caso di diffusione virale è difficile la rimozione o correzione su tutti i siti e i tempi sono lunghi. Il diritto all'immagine, da far valere di fronte al garante della privacy, soffre degli stessi problemi. Si può cambiare nome, come aveva cercato di fare anche Tiziana Cantone, ma il rischio è di creare un effetto boomerang nel caso qualcuno scoprisse del cambio. E c'è l'oscuramento del sito, la soluzione più drastica: «Ma se davvero funzionasse a dovere - dice l'avvocato Micozzi - chi distribuisce film e musica non avrebbe più i problemi di violazione delle leggi sul copyright che tutti conoscono».

> Oblio, privacy, cambio di nome: non sempre sono utili per evitare conseguenze
>
> **Francesco Micozzi**
> Avvocato del Circolo dei Giuristi Telematici

Ma allora è impossibile sfuggire al meccanismo infernale di Internet? «No - spiega ancora l'avvocato - agendo per tempo è possibile limitare i danni. Anche se, come sempre, il problema non è il mezzo - Internet - ma chi lo usa».

Ogni causa fa storia a sé, ma gli effetti sono simili. Tiziana Cantone era maggiorenne, ha acconsentito a farsi filmare, ha condiviso il video. Poi, le conseguenze, hanno travalicato le sue intenzioni, fino a diventare un incubo. Ed è la facilità con cui precipitano le cose a dover far riflettere. «Una delle mie clienti è una ragazzina di appena 12 anni. Ha postato delle sue foto a quello che riteneva il suo fidanzatino, coetaneo, che le ha condivise su Internet. Sono state rimosse, il danno psicologico però è rimasto. Chi ne risponde, essendo minore anche la controparte?».

Ci sono poi casi di totale inconsapevolezza. «Un'altra mia cliente ha una quarantina di anni. Qualcuno ha indicato, sotto una serie di video di una pornoattrice che le assomiglia, il suo nome e il suo numero di cellulare. Ci sono voluti due anni per capire cosa era successo, lei continuava a ricevere telefonate da sconosciuti con proposte sessuali, ne riceveva fino a 240 al giorno». [RAP.ZAN.]

LA STAMPA

Data 15-09-2016
Pagina 3
Foglio 1

Intervista

RAPHAËL ZANOTTI

L'allarme del garante per la privacy "Ammettiamolo, la tutela è impossibile"

Soro: "Introdurre l'educazione civica digitale tra le materie scolastiche"

«Possiamo parlare della maggiore o minore efficacia degli strumenti, della lentezza dei giudici o degli organi di controllo, però bisogna anche essere onesti: la tutela di una persona che finisce in un meccanismo del genere è praticamente impossibile». Il primo moto di Antonello Soro, garante per la privacy, è di compassione, pena, indignazione di fronte al caso di Tiziana Cantone, la 31enne che martedì si è tolta la vita perché perseguitata dal filmino hot diffuso su internet.

Dottor Soro, ma non c'era il diritto all'oblio?

«C'è ed è tutelato, ma non sempre basta a eliminare le conseguenze provocate da una diffusione virale e non risolve il problema che è a monte e che è il vero motore di questi drammi».

Cioè?

«La prima questione è quella della consapevolezza delle insidie che affrontiamo ogni volta che consegniamo alla Rete pezzi sempre più importanti della nostra vita privata. Una consapevolezza carente».

La seconda?

«È la ferocia e la violenza della nostra società. I social network sono lo specchio della mancanza di rispetto nei confronti delle altre persone, il continuo calpestare la dignità degli altri. È una questione che viaggia in parallelo con il diritto alla privacy: quando riguarda noi, lo difendiamo con le unghie e con i denti. Quando riguarda gli altri...».

E il diritto all'oblio è impotente contro questa violenza?

«Il diritto all'oblio ci pone interrogativi più generali, ma interviene sul mezzo - Internet - non sulle persone che popolano internet. Si può certamente cancellare, correggere errori pubblicati in rete, ma è impossibile una rimozione totale se prima non si interviene sul livello di odio e sull'invasione della sfera privata delle persone».

Qualcuno potrebbe dire: però è stata lei a farsi fare quei filmati...

«E qui torniamo alla questione iniziale, quella della consapevolezza. Senza quest'ultima, è un errore che poteva capitare a chiunque. Poi, però, la vicenda ha assunto dimensioni tali da diventare difficilmente affrontabile con i normali strumenti di tutela».

È difficile eliminare un video da una piattaforma in rete?

«In passato alcuni grandi social network o piattaforme si sono sottratti alle proprie responsabilità, ultimamente sono diventati più collaborativi. È un tema però complicato che oscilla su posizioni estreme: penso per esempio alle recenti polemiche sull'utilizzo di un algoritmo che censura la foto storica di Kim Phuc della bambina che scappa dall'attacco al napalm in Vietnam perché la riconosce come possibile foto pedo pornografica e al prendere tempo di un social network di fornire alla Procura di Milano le conversazioni di due terroristi che poi sono fuggiti».

Torniamo alla vicenda di Tiziana Cantone: detto che tutti rischiano di finire in un meccanismo del genere e che gli strumenti di tutela a volte non bastano, come ci si può difendere?

«Educando. Non sono favorevole a divieti e soluzioni neoluddiste. L'era digitale non è una prospettiva, ci siamo già dentro. E non è distinta dalla realtà, anzi è sempre più la realtà. Ritengo che sia utile preparare le generazioni future introducendo la materia di educazione civica digitale fin dalla prima elementare».

Insegnare dunque sia a essere prudenti nell'utilizzo di Internet sia a non aggredire quando si è dall'altra parte?

«Esattamente. Perché purtroppo, quando si agisce con gli altri strumenti, purtroppo a volte ormai la tragedia si è già verificata».

L'oblio non basta, bisogna combattere la ferocia della società I social network sono lo specchio della mancanza di rispetto

Antonello Soro
Garante della Privacy


L'allarme del garante per la privacy "Ammettiamolo, la tutela è impossibile"
Come ci si può difendere

QN
IL GIORNO il Resto del Carlino LA NAZIONE

Data 15-09-2016
Pagina 1
Foglio 1

IL COMMENTO

di GIUSELLA FINOCCHIARO

LA PRIVACY INVIOLABILE

LA DISTINZIONE *fra reale e virtuale non ha più senso in un mondo in cui comunichiamo e ci esprimiano con tutti gli strumenti a disposizione, ma la dignità della persona, alla base dei diritti fondamentali dell'uomo come riconosce anche la Carta Europea, sembra avere perso ogni significato. Vicende angoscianti quelle delle ultime ore, che hanno visto come protagonista il web. Tiziana Cantone si è tolta la vita a causa della diffusione di video intimi in rete. Una ragazza di 17 anni violentata in discoteca a Rimini in condizioni di incapacità, come si è letto sui giornali, è stata filmata, nei momenti in cui si consumava l'abuso, dalle – presunte – amiche. Al di là dei sentimenti di cordoglio, angoscia, indignazione che il lettore prova (o dovrebbe provare) leggendo simili notizie, alcune considerazioni tecnico-giuridiche si possono svolgere, sulla base delle prime informazioni ricavate in queste ore dai media. Fughiamo subito ogni dubbio: la trasmissione di contenuti personali a un conoscente o a un amico non implica un consenso tacito alla diffusione o alla divulgazione di quei contenuti.*

[Segue a pagina 2]

IL COMMENTO

di GIUSELLA FINOCCHIARO

LA PRIVACY INVIOLABILE

[SEGUE DALLA PRIMA]

NÉ UN'IMMAGINE *o un video su web sono per ciò stesso disponibili e riutilizzabili. Chi riceve una foto o un video di un terzo non è libero di fare, con quel video, ciò che vuole. Divulgare contenuti personali altrui può in astratto configurare sia un illecito penale (ad esempio, diffamazione) sia un illecito civile. Colui che ha illecitamente immesso sul web video intimi altrui senza il relativo consenso, peraltro richiesto in forma scritta dal codice in materia di protezione dei dati personali, viola non solo la normativa posta a tutela della privacy, ma anche le norme del codice civile in tema di diritti della personalità e responsabilità civile, causando un danno alla persona – sia nella sfera psicofisica, sia nella quotidiana vita sociale – che può dare luogo al risarcimento del danno patrimoniale e del danno non patrimoniale. Venendo al caso di Rimini, il fatto che oggi tutti, o quasi, abbiano uno smartphone dotato di telecamera non deve indurre a ritenere esistente una indiscriminata 'libertà di filmare' tutto ciò cui ci capita di assistere. Anzi. Occorre innanzitutto il consenso della persona ripresa. Nemmeno prospettabile nel caso di specie, dal momento che la persona era incapace (si è letto per ubriachezza) e minorenne.*

NATURALMENTE *spetterà al pubblico ministero formulare delle ipotesi accusatorie – si è letto dell'istigazione al suicidio nell'evento di Napoli –, ma la prospettazione del caso lascia immaginare che siano molteplici i reati che potrebbero ipotizzarsi. Dalla detenzione di materiale pedopornografico, all'omissione di soccorso, alle interferenze illecite nella vita privata (filmare situazioni intime di un terzo senza il consenso dell'interessato), sino all'ipotesi più estrema di concorso morale nel reato. Come ci si può difendere? Richiedendo la cancellazione della notizia o del video ai provider e ai social (quello che impropriamente viene chiamato diritto all'oblio). L'avvocata di Napoli c'era riuscita, ma ormai gli effetti psicologici devastanti si erano già prodotti. Più che mai in questi casi, il rischio è che il provvedimento risulti inefficace perché giunto troppo tardi, «come la medicina lungamente elaborata per un malato già morto», come scriveva Calamadrei. Ma quello che davvero in queste vicende sembra mancare è la consapevolezza delle azioni che si compiono (o che si omettono) dentro e fuori dal web.*


QN IL GIORNO
Quotidiano Nazionale
Donna suicida, follia web
LA PRIMA della CLASSE


ABUSI ON LINE
Video hot, indagine sul suicidio «Una condanna l'ultimo schiaffo»
«Ora è il momento del silenzio»

Il Sole 24 ORE

Data 15-09-2016
Pagina 1
Foglio 1

Privacy e dignità poco difese al tempo della Rete

Il profilo giuridico. Strumenti poco efficaci

di **Carlo Melzi D'Eril**
e **Giulio Enea Vigevani**

Ha scosso molti il suicidio della ragazza protagonista di un filmato a sfondo sessuale, che avrebbe dovuto restare privato, e che invece è stato diffuso con tale ampiezza in rete da renderla nota proprio per questo video. Ciò induce a interrogarsi su quali siano gli strumenti di difesa previsti dall'ordinamento per chi è vittima di condotte simili.

La pubblicazione senza consenso di immagini del genere, destinate a rimanere nell'intimità dei protagonisti, comporta la commissione del delitto di diffamazione aggravata dal mezzo di pubblicità, nonché quello di illecito trattamento di dati personali.

In entrambi i casi si tratta di reati di media gravità: il primo punito con la reclusione da sei mesi a tre anni o la multa e il secondo con la reclusione da sei a ventiquattro mesi.

Per giungere a una eventuale condanna e a un risarcimento, però, la persona offesa deve attendere che siano svolte le indagini e celebrato un processo, e per questo occorrono anni. È tuttavia senza dubbio possibile, e in tempi brevissimi, ottenere il sequestro preventivo dell'immagine o del video.

Se non si vuole seguire la via del diritto penale, ma si cerca "soltanto" di eliminare il materiale dal web, ci si può rivolgere al giudice civile o al Garante della privacy. Sia il primo sia il secondo possono emettere provvedimenti che impongano la cancellazione del contenuto da un qualunque sito Internet.

Questi, in termini estremamente sintetici, sono gli strumenti che l'ordinamento mette a disposizione per consentire alla persona di rientrare nel pieno controllo dei propri dati personali, "intoccabili" senza consenso o interesse pubblico.

In astratto potrebbe sembrare un armamentario sufficiente e ben attrezzato; in verità bisogna ammettere che non sempre l'interessato riesce a difendersi adeguatamente.

E ciò, ci pare, per l'esistenza di almeno due problemi.

Il primo è giuridico e riguarda l'efficacia dello strumento utilizzato: una volta ottenuto il sequestro o il blocco del filmato, non è sempre semplice oscurare in rete tutte le pagine in cui esso può comparire. Tenuto conto di quanto sia agevole oggi, per chiunque, pubblicare on-line, è intuibile come l'esercizio del proprio diritto rischi di risolversi in un vano inseguimento. Tanto che probabilmente tali contenuti sono sfuggiti al controllo anche di chi li ha diffusi sul web per primo. In più, qualora si riesca a ottenere un provvedimento d'urgenza, la sua esecuzione può essere facile solo se il sito sorgente collabora. Se viceversa non lo fa, e magari è situato all'estero, diventa tutto più difficile.

Il secondo problema è più di natura sociale e discende forse dalla scarsa consapevolezza di quanto gravi possano essere gli effetti di simili comportamenti. Pubblicare senza consenso il video di una persona mentre compie un atto sessuale, rendendola riconoscibile, rischia di incidere profondamente sulla sua dignità. Un simile atto può condurre alla spoliazione non solo del corpo ma anche dell'essenza dell'individuo che, trattato al pari di una "cosa", viene trascinato nella piazza elettronica per essere esposto al pubblico ludibrio.

L'azione di immettere tali contenuti in rete ci pare implicare un disprezzo, solitamente delle donne, che sembra quasi aizzare gli utenti non solo a guardare il video, ma anche a insultare la vittima. E forse è questo domino di conseguenze che determina, in ultima analisi, il sentimento di perdita della dignità che nei casi più drammatici può indurre a gesti tragici.

LA STAMPA

Data 16-09-2016
Pagina 11
Foglio 1

Tra i cacciatori di crimini sul web "Quando le vittime si vergognano è più difficile scovare i colpevoli"

Al lavoro 76 sezioni di polizia, innumerevoli i siti da controllare "Decisivo agire subito, sui filmati virali siamo quasi impotenti"

Reportage

MARIA CORBI
ROMA

Sexting, sex extortion, trolling. Il vocabolario dei pericoli della rete aumenta le sue pagine e la polizia postale aumenta il suo lavoro. Oltre alla sede centrale di Roma sono 20 i compartimenti e 76 le sezioni che in tutta Italia si occupano tra le altre cose dei crimini del web ma anche del suo utilizzo distorto. Tanti i ragazzini che denunciano un abuso, sempre di più da quando è stata incrementata l'azione di prevenzione. Cinquecentomila i ragazzi che lo scorso anno hanno partecipato a eventi informativi .

Ma cadere nei tranelli della rete e dei social non è solo una cosa da ragazzi, tanti anche gli over 40. Aumenta il lavoro dei poliziotti che si dedicano ai crimini virtuali. E se le emergenze su cui si concentrano rimangono il terrorismo e la pedopornografia, quel che accade sui social assorbe molte delle loro energie.

Nessun commento sulla vicenda di Tiziana «uccisa» da quel video hot che lei stessa aveva condiviso su WhatsApp. Indagini in corso. Quando invece la vittima è una minorenne la polizia postale procede immediatamente, altrimenti occorre formalizzare una denuncia. Passa del tempo, una variabile importante, e le cose si complicano. In ogni caso gli individui che hanno condiviso una foto «sensibile» oggetto di denuncia sono rintracciabili anche se il passaggio è avvenuto via WhatsApp e via Snapchat.

«Il problema è che spesso le persone si vergognano e tendono a non fornire tutti gli elementi utili per darci una mano», dice uno degli ispettori che ogni giorno affronta emergenze del genere.

Tante le ragazzine vittime del sexting - neologismo derivante dai termini inglesi sex e texting (mandare messaggi a sfondo sessuale) - ma soprattutto della sex extortion, spiega Carlo Solimene, dirigente della divisione investigativa della Polizia postale, ossia «l'immissione di immagini in rete con finalità estorsive». Una ragazzina chatta con un coetaneo che le chiede, per esempio, di spogliarsi e poi la ricatta con la minaccia di diffondere quelle foto. Lo scambio può essere anche non in denari ma solo con compiti di scuola, una versione, un tema. Oppure c'è la «revenge porn», nel caso in cui un ex condivide per vendetta momenti intimi e imbarazzanti sulla rete.

«Noi consigliamo sempre di non pagare - dice Solimene -. Siamo in grado di congelare questa immagine e di rimuoverla dalla rete solo nell'immediatezza dei fatti, quando la rete non ha prosciugato quell'immagine. Se invece la foto è viralizzata, ossia ha girato su tutti i siti, possiamo rimuoverla con un decreto di rimozione del magistrato, ma se qualcuno l'ha conservata in memoria, allora potrà sempre riuscire fuori».

Insomma un invio di immagini alla persona sbagliata può tormentarci tutta la vita. E non c'è attività investigativa che tenga. «Per evitarlo dobbiamo non immettere in rete foto che consideriamo private e che non vogliamo che siano viste». Le ragazzine divulgano le foto senza pensare che alla fine quello scatto innocente potrà arrivare in rete attraverso una catena di clic, e magari arrivarci taroccata.

«Il poliziotto prima di tutto fa prevenzione - insiste l'esperto -. Capire questo è fondamentale, perché quando la frittata è fatta allora non rimane che andare alla procura della Repubblica». Anche quando si tratta di trolling, ossia della «pesca alla traina» su internet di una vittima da sopraffare in gruppo.

Molti ragazzi sulle strade del cyberbullismo credono che facendo minacce attraverso un computer, o divulgando immagini, non possano essere identificati. «Invece sicuramente verranno identificati - spiega Solimene -. E spesso quel computer porta ai loro genitori che si troveranno sulle spalle una bella denuncia».

Un mondo in continua evoluzione, quello del web e dei social, che richiede un continuo aggiornamento di chi deve contrastarne il cattivo utilizzo o il crimine. WhatsApp e Snapchat sono ormai roba da «matusa», le nuove applicazioni di condivisione si chiamano WeChat, Tango, Hike e Yuilop. Poi c'è Hide It Pro che serve a nascondere foto, testi e video. La polizia postale «insegue» queste novità. Forse però anche i genitori dovrebbero iniziare a correre.

QN
IL GIORNO Il Resto del Carlino LA NAZIONE

Data 16-09-2016
Pagina 5
Foglio 1

Colossi Internet e contenuti illegali «Ora basta, li rimuovano in fretta»

Il Garante per la privacy: ma la legge non prevede loro responsabilità

Alessandro Belardetti

«La giustizia ordinaria ha tempi troppo lunghi e il fattore temporale, nella rimozione dei contenuti lesivi della dignità altrui o illegali, è decisivo. È necessario che i social velocizzino le procedure di risposta per effettuare interventi più efficaci». Il presidente dell'autorità Garante per la privacy, Antonello Soro, individua nella tempestività del sistema di rimozione di messaggi, foto e video un punto cruciale per prevenire tragedie come quella di Tiziana Cantone. «Ma l'aspetto fondamentale è la sensibilizzazione degli utenti, che non sono consapevoli di diffondere materiali intimi a un'infinità di persone e, nell'illusione di anonimato, usano un linguaggio feroce, fino all'insulto».

Il sogno del social come diario innocente è durato troppo poco.

«Se un soggetto economico con un miliardo e mezzo di clienti compra un'azienda con un miliardo di clienti (WhatsApp, *ndr*) l'idea romantica del social fra vecchi compagni di Liceo cambia. Tuttavia, non penso che gli aspetti distorsivi siano colpa dei gestori delle piattaforme, bensì degli internauti, sprovvisti di educazione digitale».

Essendo i social mezzi di comunicazione, perché non vengono sanzionati quando consentono la pubblicazione di contenuti fuorilegge?

«Nel nostro ordinamento, in linea generale, i social non sono responsabili dei contenuti pubblicati dai propri utenti. Tuttavia, dopo una prima fase di chiusura, adesso anche i cosiddetti Over The Top hanno capito che è nel loro interesse cercare di rendere più sicura la piazza virtuale. Per questo, stanno cominciando a collaborare e hanno accettato di usare forme automatiche di rimozione dei contenuti d'odio o pedopornografici. Ma c'è ancora molto da fare».

Quali sistemi vengono usati per filtrare i file postati in Rete?

«Principalmente algoritmi filtr per parole e foto chiave che, pur imperfetti, svolgono un ruolo utile. Ma non illudiamoci: se un video viene rimosso anche dopo cinque minuti, in quel lasso di tempo potenzialmente è già diventato virale. Spesso, poi, la parte lesa ne viene a conoscenza molto tardi e la frittata è fatta».

Esiste un'arma contro i profili falsi, creati da bimbi e ragazzini che non avrebbero l'età per iscriversi?

«Purtroppo, lo strumento proposto per individuarli consisterebbe nella sorveglianza continua di tutti i loro comportamenti sul web. Ma questo comporterebbe il rischio ancora più grande di una profilazione di massa, in realtà estesa a tutti gli utenti. E, l'idea di subordinare l'iscrizione alla presentazione di un documento consegnerebbe ai gestori una sorta di anagrafe universale. Una follia».

Le modifiche alla legge sul cyberbullismo la convincono?

«È presto per giudicarla, certo ha subito molti cambiamenti. L'intenzione dei proponenti, comunque, è condivisibile per rendere più efficiente la prevenzione di fenomeni pericolosi».

Alzare l'età minima per accedere ai social sarebbe una misura per prevenire potenziali tragedie?

«Molti fingerebbero comunque di avere 18 anni, se fosse l'età minima. Precludere un social fino ai diciotto anni significa andare contro alla qualità della vita che si è creata. Quello che invece sarebbe utile è investire sull'educazione civica digitale, sin dalle Elementari, per far capire ai bambini quali sono i rischi. In Estonia è una materia scolastica sin dalla prima elementare».

EDUCAZIONE DIGITALE

«Bisogna fare investimenti per insegnare ai bambini tutti i rischi della Rete»


Colossi Internet e contenuti illegali «Ora basta, li rimuovano in fretta»
ecco come ripulisco i profili violati

ItaliaOggi

Data 16-09-2016
Pagina 1
Foglio 1

Per il Garante non c'è bisogno dell'autorizzazione sindacale per l'uso in azienda o nella pubblica amministrazione

Privacy, il software è senza vincoli

Posta elettronica, internet e software applicativi sono strumenti di lavoro e non hanno bisogno dell'accordo sindacale per essere utilizzati in azienda e negli enti pubblici. Non sono strumenti di lavoro, invece, apparati e applicativi che non toccano le mansioni e con i quali, in background, costantemente e indiscriminatamente si filtrano, monitorano, controllano e tracciano gli accessi a internet e alla posta elettronica. Lo ha chiarito ieri il Garante privacy.

Ciccia Messina a pag. 34

Patronati ispezionati

Patronati relativamente al 730 precompilato, telemarketing e call center; concessionarie di giochi online; sistemi informativi dell'Istat; società di ristrutturazione del debito. Sono questi alcuni dei settori interessati dalle ispezioni del garante privacy nel secondo semestre 2016 (provvedimento 327 del 28/7/2016). Intanto un bilancio del primo semestre 2016 registra un'impennata delle sanzioni. Le somme già riscosse sono state pari a circa 1 milione e 900 mila euro (con un aumento del 5% rispetto al primo semestre 2015). Le sanzioni contestate sono state oltre 2.000 (con un aumento del 44% rispetto al primo semestre dello scorso anno). 37 sono state le segnalazioni all'autorità giudiziaria (+85% rispetto al primo semestre 2015) che hanno riguardato soprattutto casi di mancata adozione delle misure minime di sicurezza, le violazioni connesse al controllo a distanza dei lavoratori, l'inosservanza dei provvedimenti del garante. Per quanto riguarda le misure minime di sicurezza sono state impartite complessivamente 26 prescrizioni, tra soggetti pubblici e privati.

SPOT IN TV. Sky può utilizzare i dati dei propri utenti per inviare spot pubblicitari mirati a spettatori di uno stesso programma, ma solo in forma aggregata. I destinatari della pubblicità sono i nuclei in possesso di uno specifico apparecchio per la ricezione da satellite o via internet, raggruppati in appositi cluster in base al servizio fruito (tipologia del pacchetto tv, durata dell'abbonamento, modalità di pagamento) e ad altre informazioni (fascia di età, luogo di residenza). Tuttavia l'utente che non intende ricevere questi spot può però opporsi in modo semplice, anche usando il telecomando. Lo ha stabilito il garante privacy (provvedimento 306 del 13/7/2016), accogliendo una richiesta di verifica preliminare presentata da Sky e relativa alla realizzazione di un progetto mediante il quale la società intende veicolare altri messaggi pubblicitari, al posto di quelli standard, a gruppi differenti di spettatori ciascuno dei quali con caratteristiche ben definite.


ItaliaOggi

Ici, la Chiesa assolta dall'Ue

Privacy, il software è senza vincoli

RIMBORSI FISCALI


LAVORO E PREVIDENZA

Il software strumento di lavoro

L'utilizzo degli applicativi senza accordo sindacale

Patronati ispezionati

CORRIERE DELLA SERA

Data 19-09-2016
Pagina 19
Foglio 1

Video e ricatti Come difendersi

Canali «a scomparsa» e norme sulla privacy Quali cautele adottare e a chi rivolgersi in caso di trappole online

Un gioco, sessuale prima e di condivisione poi, può trasformarsi in un pericoloso boomerang. E un boomerang lanciato in Internet, si tratti di social network o di applicazioni di messaggistica, inizia a ruotare a una velocità che aumenta esponenzialmente con il passare delle ore e dei clic. Il mezzo, ovviamente, non ha responsabilità ma, per sua stessa natura, consente ai contenuti e ai commenti di ogni tipo di rimbalzare in una modalità senza uguali nella storia. E con cui si deve fare i conti sia in termini di opportunità sia di rischi.

Dai telefoni al web

Una pellicola di un paio di anni fa, «Sex tape - Finiti in Rete», ha divertito gli spettatori delle sale cinematografiche con le vicissitudini di una coppia che scopriva di aver pubblicato per errore una performance sessuale in un cloud collegato a una serie di dispositivi. Ecco: non c'è niente da ridere. Se fatti per uso personale, foto e video vanno tenuti lontano dalle piattaforme connesse alla Rete. Nel caso in cui li si voglia condividere, bisogna tenere a mente che la diffusione impazzita parte da singoli utenti: è bene inviarli, quindi, solo a persone fidate (evitare sconosciuti e flirt online o offline), e usare canali con la funzione a scomparsa.

Meglio Snapchat, che avvisa anche di eventuali tentativi di salvare il contenuto da parte di chi lo riceve, di WhatsApp. Negli scatti e nelle riprese destinati a viaggiare da uno smartphone all'altro, è inoltre fondamentale assicurarsi di non essere riconoscibili. Il vero dramma di Tiziana Cantone, la 31enne che si è tolta la vita il 13 settembre, è stata la circolazione del suo volto, del suo nome e delle frasi pronunciate con la sua voce.

Rivolgersi al Garante

Se gli accorgimenti non sono sufficienti e ci si ritrova alla mercé di chiunque, il consiglio è di «identificare gli indirizzi di pubblicazione dei contenuti e passare in rassegna i gestori delle piattaforme. Difficilmente le autorità compiono queste operazioni e così facendo si riducono i tempi di intervento», spiega l'avvocato esperto di diritto digitale Guido Scorza. Il primo tentativo da fare è con le piattaforme stesse: «Davanti a una segnalazione della Url hanno tutto l'interesse a procedere con la rimozione per evitare problemi». Contemporaneamente, per accorciare i tempi, conviene rivolgersi a un'autorità competente: «Il Garante per la privacy è preferibile, ha maggiore dimestichezza con la materia e meno casi da affrontare rispetto alla giustizia ordinaria (civile, ex articolo 700, o penale, *ndr*)». Anche perché «la norma di riferimento è il Codice per la privacy, quantomeno inizialmente. E non è importante il consenso concesso alla diffusione dei dati personali: anche nel caso in cui si presume sia stato dato, è comunque sempre revocabile».

I riferimenti per il ricorso all'Authority sono disponibili online, come online si può avviare l'iter di denuncia alla Polizia. Per quello che riguarda la legislazione, è diverso il discorso del diritto all'oblio cui si può fare riferimento in un eventuale secondo momento per non rendere rintracciabili gli articoli sulla storia considerata lesiva dalla propria immagine. Non ha che fare con i video da rimuovere, ma con quello che può essere poi pubblicato in merito, insomma.

Cosa fare con i figli

I dati parlano chiaro: un adolescente su dieci conosce qualcuno che ha mandato messaggi con foto e video sessualmente espliciti (fonte: Telefono Azzurro) e il 10%, dei dirigenti scolastici si è trovato a dover gestire un caso del genere (fonte: Censis).

«I genitori non devono avere un approccio repressivo o tentare di controllare quello che viene pubblicato. Bisogna utilizzare e conoscere le piattaforme — tutte, non solo Facebook — in modo da poter spiegare ai figli come tutelarsi. Scambiamo la praticità e capacità di apprendere dei ragazzini con reale conoscenza dei mezzi, in materia di privacy ad esempio», spiega Paola Brodoloni, presidente di Cuore e Parole Onlus. L'associazione è presente dallo scorso anno scolastico negli istituti con il progetto «Scelgo io!» per dare ai docenti materiale utile per affrontare il tema. L'aspetto della formazione nelle scuole fa parte anche nella proposta di legge sul cyberbullismo già approvata al Senato e attualmente alla Camera.

Martina Pennisi
@martinapennisi

IL MATTINO

Data 23-09-2016
Pagina 11
Foglio 1

«Colossi inafferrabili ma anche ritardi dei giudici ora leggi Ue per obbligare i social a rispondere»

Intervista

Sica, prof di Diritto all'informazione all'Università di Salerno: impossibile di fatto tracciare l'iter dei dati

Web e privacy: la disamina di Salvatore Sica, ordinario di Diritto privato all'università di Salerno, tra i massimi esperti italiani in materia di diritto dell'informazione e della comunicazione, è lucida e tagliente.

Professore, quali effettive possibilità ha la persona che si sente lesa, di difendersi dalla gogna sul web?

«Verrebbe da rispondere, d'istinto, nessuna! Al tempo della rete e dei social la privacy, di fatto, non esiste più sicché la sola garanzia di rispetto della propria vita personale è non condividere i propri dati, informazioni, immagini con nessuno a meno di non avere l'illusoria certezza che non saranno diffusi. Sì, perché il punto è questo; spesso si condivide con una comunicazione - per capirci, da soggetto a soggetto - un dato, ma poi esso è fatto oggetto di diffusione, cioè trasferito in una comunità indistinta ed incontrollabile. Da quel momento in poi il controllo dei dati è "perso" per sempre. Ciò è ancor più vero se si considera che i "gestori del traffico", i colossi del web, negano di poter intervenire e tracciare il percorso dei dati: costringerli a dar conto di questa affermazione sarebbe già un bel passo avanti».

Tiziana Cantone è stata condannata a pagare le spese processuali: come è potuto accadere?

«Occorrerebbe leggere integralmente il provvedimento; se, come pare, la condanna sia avvenuta a favore di alcune delle grandi multinazionali della rete, esso lascia fortemente perplessi, sia rispetto al diritto di internet, ancora pieno di incertezze, sia con riferimento all'utilizzo in sé della condanna alle spese legali: andrebbe usata con maggiore attenzione alla natura controversa delle questioni. Ma, ripeto, andrebbe verificata la logica che il giudice ha certamente seguito, perché vista dall'esterno, appare soltanto una decisione "esemplare" che rischia di corroborare nelle multinazionali l'idea di essere intoccabili, con l'avvertenza che nessuno s'azzardi addirittura a convenirle in giudizio».

Quali sono le difficoltà più comuni nell'ambito di un processo per diffamazione che veda coinvolti social e loro utenti?

«La prima è la non tempestività; il ritardo dell'intervento delle procure è un problema generale, che crea sfiducia nelle giustizia in senso più ampio; si figuri in un ambito in cui il tempo di intervento è tutto, oltre ai noti problemi, che spesso hanno gli stessi inquirenti, di seguire l'iter dati: ribadisco, vanno responsabilizzati i soggetti che sui click fanno affari, i gestori della rete. Sa chi guadagna sui contatti ai siti che contengono le foto "strappate"? I gestori stessi dei siti. Finché non si comprende che ciò che per ognuno di noi è dato personale per questi soggetti è dato economico non ne verremo a capo».

Spesso i maggiori social si dichiarano irresponsabili per i contenuti...

«I colossi della rete vanno obbligati per legge sovranazionale a radicarsi in ogni singolo paese in cui operano: non si può consentire loro di replicare di essere americani in Italia, di Singapore a Londra e così via. E questo deve valere anche sul piano fiscale».

Che fare in assenza di leggi efficaci?

«Urge un'opera innanzitutto educativa, ma noi viviamo un tempo di "droga collettiva" da abuso della comunicazione". Se scuole, parrocchie e così via, oltre ad usare i social, educassero ad usarli, sarebbe meglio. Non è detto che servano nuove leggi, basterebbe usare meglio quelle che ci sono. E superare l'idea che se si tocca la rete si attenta alla libertà di opinione: non è sempre così. L'esaltazione del "mezzo" ha oscurato la consapevolezza del pericolo sui e dei contenuti. Il rischio è che sia già troppo tardi con un potere in mano a privati come mai in passato: oggi le autorità pubbliche chiedono aiuto ai gestori della rete e non il contrario: questa è la vera emergenza democratica».

f.l.d.


Primo piano 11

Tra moglie e marito c'è di mezzo anche la Rete

«Colossi inafferrabili ma anche ritardi dei giudici ora leggi Ue per obbligare i social a rispondere»

Il Sole 24 ORE

Data 24-09-2016
Pagina 19
Foglio 1

Domande e risposte. Identità digitali a rischio

Il vademecum per difendersi. Primo: cambiare password

Di che dimensioni è il furto informatico di dati subìto e denunciato da Yahoo?
I dati di mezzo miliardo di utenti sono stati sottratti a Yahoo! e messi in vendita sulla dark net. Sono numeri che lo hanno già fatto ribattezzare il furto informatico più grande della storia. Numeri che tradotti in denaro diventano un danno incalcolabile per l'azienda di Sunnyvale, alle prese – tra l'altro – con una mega operazione di vendita a Verizon per 4,8 miliardi di dollari. E non è un caso che proprio da Verizon, qualche ora dopo l'ammissione di Yahoo!, abbiano espresso forti perplessità riservandosi ogni decisione per tutelare azionisti e utenti. Operazione di cessione a rischio? Difficile dirlo adesso. Si vedrà.

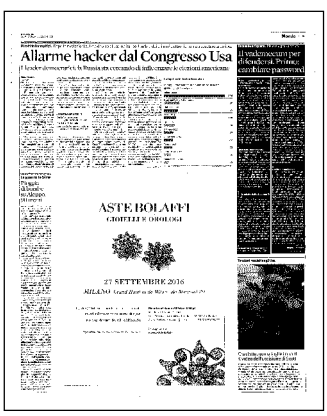
Quali sono i dati a rischio?
Per ammissione della stessa società guidata dal Ceo Marissa Mayer, con l'attacco informatico (che risale al 2014) sono stati sottratti nomi, indirizzi email, numeri di telefono, date di nascita e password di oltre 500 milioni di persone. Dati che, in una veduta più ampia, mettono a rischio miriadi di identità digitali. Non sarebbero finiti nelle mani dei cyber criminali, invece, i dati bancari e relativi alle carte di credito.

Chi ha rubato i dati e dove sono finiti?
La montagna di informazioni rubata a Yahoo! è finita sulla dark net, l'insieme di siti Internet non raggiungibili con una comune ricerca online, ma solo attraverso software come Tor. Si tratta del web sommerso, dove i dati di una carta di credito sono in vendita a pochi euro, come la frutta al mercato rionale. Difficile, invece, dare un'identità al colpevole. Almeno per ora. Yahoo! ha parlato di gruppo hacker pilotato da uno Stato straniero, ma è una posizione che non convince gli esperti.

Cosa fare in quattro passaggi?
Chiunque sia in possesso di un account Yahoo! può cercare di tutelarsi seguendo quattro passaggi chiave. Primo: cambiare le password. Non solo quella dell'account Yahoo!, ma tutte le password degli account online. Questo perché molto spesso si usa la stessa password per accedere a vari siti. Secondo: entrare nel proprio account Yahoo! ed eliminare le email contenenti dati sensibili, ricordandosi di svuotare il cestino. Terzo: aprire un account di posta elettronica sotto un dominio più sicuro e attivare o la doppia autenticazione che passa da un sms sul cellulare, o una chiave PGP in modo da cifrare ogni tipo di dato o file così che solo il destinatario della mail possa leggere il contenuto. Quarto: non aprire email strane. Inoltre - su suggerimento degli esperti di Kaspersky Lab - se si utilizza un account di posta elettronica Yahoo «è una buona idea applicare la "Yahoo account key", che elimina la necessità di inserire password e consente un livello di autenticazione in due step».

Perché due anni dopo?
Fa discutere, inoltre, la tempistica con la quale Yahoo! ha comunicato l'attacco. Due anni di distanza sono veramente tanti. «Gli Stati Uniti, dove Yahoo! ha la propria sede, hanno una legislazione differente da quella europea e da quella dei singoli Stati Ue – ci dice Gabriele Faggioli, responsabile scientifico dell'Osservatorio Information Security & Privacy del Politecnico di Milano e presidente del Clusit -. In California, Yahoo! non sarà tenuta a notificare la violazione dei dati agli interessati, non sussistendo tra i dati rubati informazioni finanziarie. In Italia c'è l'obbligo di comunicare eventuali violazioni al Garante, e in alcuni casi, anche ai soggetti interessati. Il mancato o ritardato adempimento della comunicazione espone alla possibilità di sanzioni amministrative».

A CURA DI
Biagio Simonetta


Allarme hacker dal Congresso Usa
Il vademecum per difendersi. Primo: cambiare password
ASTE BOLAFFI
GIOIELLI E OROLOGI
27 SETTEMBRE 2016

il Giornale

Data 24-09-2016
Pagina 1
Foglio 1 / 2

ACCOUNT VIOLATI E VIDEO RUBATI

La rivincita dei non-digitali: il web non è sicuro

di **Stefano Zecchi**

Tra i diversi conflitti generazionali, c'è anche internet. Sono un papà diversamente giovane di un ragazzino dodicenne. Per lui internet è l'essenza della vita, per me un problema della vita. Da lui vengo mortificato, deriso ogni volta che pasticcio con la posta elettronica e Google, e capisco che non ho chance per difendermi dalla sua commiserazione. Ma, in queste settimane, tutta la tradizionale generazione non digitale, che è ancora una maggioranza silenziosa, sta avendo la sua rivincita.

Un sottile, crudele piacere sta attraversando le nostre menti. Crudele perché si basa sulle disgrazie altrui, sottile perché non durerà a lungo: solo un contentino per far capire che (...)

Piccola (e crudele) rivincita per noi dinosauri digitali

Il progresso della tecnologia è inarrestabile. Mi adeguo ma gli ultimi casi dimostrano le falle di questo processo

IL COMMENTO

di **Stefano Zecchi**

dalla prima pagina

(...) noi, proprio fessi, non siamo. Non c'è bisogno di ricordare nei dettagli cosa sia successo a chi fa uso e abuso di internet. Da quella povera ragazza sconsiderata che ha messo i suoi filmini hard in rete fino al furto della privacy con l'attacco dei pirati informatici a Yahoo, è tutto un discutere sull'uso delle piattaforme elettroniche nelle loro diverse due possibilità, da quelle bancarie agli acquisti di merce, alla posta all'informazione. Indietro non si torna, e affermare che l'online sia inutile è assolutamente falso. Indiscutibile è la semplificazione di tante operazioni proprie della quotidianità - banca, posta ecc. - che prima richiedevano tempo, code estenuanti e, talvolta, anche qualche fastidioso litigio. Dunque, si vada avanti, ma come?

La risposta che ora è sulla bocca di tutti si riassume con una parola: «sicurezza». Più che comprensibile. Ognuno vuole essere tutelato da chi gli offre un servizio: se questo servizio presenta dei rischi, sia in fatto di privacy sia di tutela dei propri soldi, o quel servizio si chiude o si adegua alle esigenze richieste. Abbiamo detto - e il buonsenso non può che confermarlo - che indietro non si torna: siamo nelle mani di internet, a lui ci siamo affidati. Davvero possiamo dormire sonni tranquilli, convinti che le falle del sistema saranno riparate? Neanche per sogno. E a dirlo non sono io, per ripicca verso chi mi considera uno scettico antinformatico, ma chi è del mestiere. Viviamo nell'insicurezza: i nostri messaggi possono essere controllati; il bancomat può essere clonato; i negozi online degli imbrogli. Certo, tutto ciò è inquietante, ma anche molto affascinante. Il mondo si globalizza, si abbattono le frontiere della comunicazione, viviamo tutti nello stesso condominio, la rapidità diventa una divinità verso la quale s'inchina qualche miliardo di persone. Tuttavia, di fronte a tali conquiste, mi si permetterà di sostenere che la difesa della nostra identità, della nostra storia, della nostra tradizione, messe in soffitta dal villaggio globale, non è cosa tanto disdicevole.

Poi, per quanto mi riguarda, c'è anche una piacevole riflessione sulla tecnologia. La sua presunta infallibilità. Sembra ormai che essa usi l'uomo, lo manipoli, gli faccia fare quello che vuole. Poi, però, ci sono incidenti di percorso che fanno capire ciò che davvero deve essere per noi la tecnologia: uno strumento che non ci usa, ma che usiamo.

Ecco, quindi, il patto generazionale che propongo al mio figlioletto: io mi rendo disponibile a ogni innovazio-

ne tecnologica, lui mi lascia tutto il mio scetticismo in proposito, senza deridermi; io mi adeguo alla contemporaneità, ma lui abbassa la sua fede verso le conquiste della tecnologia informatica.


il Giornale

Da oggi in edicola col «Giornale» il volume «Storia della Turchia»

PARTITE IVA

Tutto sulla nuova tassa

Da Merkel e Hollande foglio di via a Renzi

Ecco le vere macchine del fango


Piccola (e crudele) rivincita per noi dinosauri digitali

PEUGEOT 308

Il Messaggero

Data 30-09-2016
Pagina 20
Foglio 1

Piano nazionale di cybersecurity Finmeccanica scende in campo

▶Moretti e Alfano: «Indispensabile fare sistema contro la pirateria informatica»

IL CONVEGNO

ROMA Il ministro degli Interni Angelino Alfano e Mauro Moretti, ad di Leonardo Finmeccanica, sono d'accordo. Serve una forte partnership pubblico privato per la cybersicurezza, una grande alleanza contro i pirati informatici, sempre più agguerriti e pericolosi. «Perché - aggiunge il direttore della Dis, Alessandro Pansa - l'Italia ha davvero bisogno di un progetto nazionale che contrasti un fenomeno in aumento, tra minacce terroristiche e furti di segreti aziendali. Al convegno Cybertech Europe 2016, si è fatto il punto, delineato strategie, individuato ricette. Soprattutto dal fronte industriale, Leonardo-Finmeccanica ha teso la mano al governo per creare una rete di protezione a tutto campo. Del resto il gruppo guidato da Moretti è tra i leader del settore: Con prodotti specifici per proteggere dal rischio intrusione non solo piccole e grandi imprese, ma anche la Pa. Da qui la richiesta di una nuova organizzazione nazionale dedicata alla sicurezza informatica sulla scia dell'«European Cyber Security Organization» recentemente costituito da Leonardo e altri partner industriali e governativi. Oggi il mercato della cybersecurity vale in Europa 25 miliardi di euro e in Italia 2,4 miliardi, con stime che indicano una crescita annua del 9%. Moretti ha spiegato che Leonardo-Finmeccanica realizzerà un report che monitorerà il grado di esposizione ai pericoli del web dei principali macro settori economici, segnalando preventivamente agli utenti, sulla base delle informazioni rilevate in rete, le potenziali modalità d'attacco e le misure da adottare per ridurre il rischio. Altra novità presentata da Leonardo è Cyber Asc. Si tratta di una polizza assicurativa per proteggere le Pmi e i professionisti dal rischio informatico. Indagini recenti evidenziano infatti come l'80% delle aziende italiane sia stato vittima di violazioni informatiche negli ultimi 5 anni e che il 33% teme che possa accadere di nuovo.

Con infrastrutture dedicate in Italia e in Europa, Leonardo è partner tecnologico di istituzioni governative e organizzazioni commerciali e finanziarie per attività di prevenzione, prima tra tutte la Nato e il ministero della Difesa della Gran Bretagna.

Umberto Mancini


Piano nazionale di cybersecurity Finmeccanica scende in campo

Il Messaggero

Data 02-10-2016
Pagina 13
Foglio 1

«Pirati informatici, serve un patto tra aziende e governi»

LA TECNOLOGIA

ROMA «In un mondo sempre più connesso a internet, per hacker e pirati informatici si moltiplicano le opportunità e, di riflesso, per singoli privati, imprese e perfino Stati si moltiplicano i rischi». E' questo, in estrema sintesi, il pensiero di Amir Rapaport, fondatore di Cybertech, tra i maggiori eventi a livello mondiale dedicato alle soluzioni cibernetiche. Il 29 settembre, al Palazzo dei congressi di Roma, in presenza di manager societari e politici (c'erano, per esempio, il ministro dell'Interno, Angelino Alfano, e l'amministratore delegato di Finmeccanica-Leonardo, Mauro Moretti) si è tenuto Cybertech Europe, evento che ha rappresentato un'occasione di dialogo internazionale sulle minacce informatiche, le esigenze del mercato e le soluzioni più innovative. «Possono essere a rischio attacco informatico - spiega Rapaport - i computer, i telefonini smartphone, ma anche altri oggetti e cose meno facilmente immaginabili, come gli aeroplani o addirittura l'elettricità. Basti pensare che gli aerei nonm sono indipendenti ma sono connessi sia ad altri aerei nel cielo sia alle strutture di terra».

NEL MIRINO

Insomma, signori e signori, benvenuti nell'era del cosiddetto Internet delle cose, in cui ognuno di noi è sempre e costantemente connesso a tutto, con i pericoli che possono conseguirne. «I rischi - fa notare il fondatore di Cybertech - si articolano su più livelli: quelli del singolo privato, che in generale deve acquisire maggiore consapevolezza per capire quali siano; quelli delle aziende, che, a seconda dell'eventuale attacco di pirateria informatica di cui sono vittime, possono mettere in serio pericolo il proprio business; e poi ci sono i Paesi, perché la sicurezza informatica deve rappresentare una preoccupazione anche politica». Tra l'altro, aggiunge Rapaport, a differenza di quanto qualcuno potrebbe essere portato a pensare, «il rischio di pirateria non deve preoccupare solo le aziende tecnologiche ma anche quelle che operano nei settori dell'industria più tradizionale». Non è un caso che al Cybertech Europe fossero presenti anche Enel e Fiat Chrysler Aumobiles, oltre alla già citata Finmeccanica-Leonardo.

NUOVA CONSAPEVOLEZZA

Le imprese, secondo il fondatore di Cybertech, devono diventare sempre più consapevoli della necessità di avviare una collaborazione tra loro. «E' necessaria - sottolinea l'esperto di sicurezza informatica - un'intensa collaborazione tra Paesi e imprese. Non è un caso che il ministro Alfano abbia rimarcato che la battaglia alla pirateria è una sfida che l'Italia deve raccogliere e che può essere vinta proprio con una maggiore collaborazione». E tutto questo con una ulteriore consapevolezza: le tecnologie ormai si muovo in tempi rapidissimi. «Un anno nel cyber - sostiene Rapaport - corrisponde all'incirca a 20 anni nell'industria tradizionale». Questo significa che, così come possono nascere nuove tecnologie sempre all'avanguardia, allo stesso modo possono nascere nuovi attacchi di pirateria informatica fino al giorno prima impensabili. Da qui non solo la necessità di essere sempre aggiornati contro i pericoli ma anche la necessità di agire contro i crimini informatici con rapidità e tempestività.

Ca. Sco.

IL FONDATORE DI CYBERTECH AMIR RAPAPORT: «NON È IN PERICOLO SOLAMENTE IL BUSINESS»


Spagna, caos socialisti: si dimette Sanchez

132

Usa, Trump in difficoltà prende lezioni da Farage

«Pirati informatici, serve un patto tra aziende e governi»

IL MATTINO

Data 04-10-2016
Pagina 1
Foglio 1 / 2

S. Maria Capua Vetere, causa archiviata: il colosso web non collabora

Se i giudici si arrendono a Facebook

Salvatore Sica

Nel dibattito che investe la tutela «in e da» Internet, purtroppo sviluppatosi in relazione ai video hot fatti circolare attraverso una chat e che nel caso di Tiziana Cantone hanno condotto al suicidio della giovane, si inserisce anche la singolare vicenda di cui diamo conto. Un cittadino decide di candidarsi alle elezioni comunali del 2016 del proprio Comune; in tale occasione sulla pagina Facebook di «tale Postiglione Marco» compaiono frasi offensive nei suoi riguardi o perlomeno che tali appaiono nella sua valutazione.

Se i giudici si arrendono a Facebook

Salvatore Sica

Nel maggio del 2016, si ritiene con tempestività, presenta querela alla Procura della Repubblica presso il Tribunale di Santa Maria Capua Vetere affinché il responsabile dei fatti sia identificato e perseguito. In data 14 settembre, a circa quattro mesi dalla querela, il pubblico ministero titolare dell'indagine, formula richiesta di archiviazione, così testualmente motivata: « Dall'esito dell'attività di indagine delegata alla polizia postale di Caserta, è emersa l'obiettiva difficoltà di pervenire all'identificazione del responsabile in quanto i gestori di Facebook sono poco collaborativi nel fornire i dati telematici se non attraverso una rogatoria internazionale che comunque deve concludersi entro 12 mesi dalla commissione del fatto poiché i dati telematici sono disponibili solo entro quel termine». Ne consegue per il pm che «sostanzialmente è emersa l'impossibilità di identificare l'autore del reato in contestazione entro il termine sopra indicato».

Il fatto ha un fortissimo valore emblematico, ben oltre la specifica vicenda da cui trae origine (del resto, archiviazioni così formulate sono assai più frequenti di quanto si immagini). La prima sensazione che si ricava è di una diffusa sfiducia nella possibilità di ottenere giustizia in un settore che, lungi dall'essere una «nicchia» della società, oggi è il crocevia fondamentale delle relazioni sociali, politiche ed economiche: internet ed il suo mondo. Se coloro che hanno responsabilità istituzionali - giudici, avvocati, classe dirigente, in senso ampio - non percepiscono che quella della Rete e della sua disciplina è un'emergenza che richiede precedenza di intervento, i rischi ed i costi potenziali sono altissimi. Del resto, viviamo un tempo in cui non rileva soltanto ciò che avviene ma piuttosto ciò che è percepito e diffuso sul piano della comunicazione; e questo vale per tutti: lasciare un reato senza colpevoli è sempre odioso, se si lo si consegna all'«eternità» mediatica è ancor più grave. Forse con un po' di sforzo gli inquirenti avrebbero potuto pensare, ad esempio, ad individuare l'IP del computer attraverso il quale si è consumato il fatto denunziato per fare un passo avanti. Certo, si sarebbe identificato una macchina e non una persona, ma il progresso investigativo sarebbe stato notevole. Ma capisco anche che in una Procura «affollata» di ben altre indagini o probabilmente «sommersa» da quotidiane querele per casi simili la soluzione dell'archiviazione per mancanza di collaborazione di Facebook è la più agevole.

In realtà, il provvedimento - e la relativa scelta del pm - manifesta tutta l'impotenza degli strumenti tradizionali del diritto rispetto alla società della rete; ed il dato preoccupante è lo scenario che è sotto i nostri occhi: viviamo travolti da flusso di dati informativi, siamo tutti immersi - autorità tradizionali incluse - in un acquario in cui abbiamo la sensazione di saper nuotare, ma se un predatore ci aggredisce alle spalle, quando ci giriamo è già scomparso, a dispetto delle ferite che restano per sempre impresse nella nostra carne. Ha ragione la Procura quando segnala che Facebook è sottoposto alla giurisdizione americana e se vuoi la sua «collaborazione» devi passare per una rogatoria internazionale ; tra l'laltro, non è detto che ciò accada, visto una legge statunitense del 1996 (governo Clinton: Communication Decency Act!) rende del tutto irresponsabili i provider di ciò che accade in rete, senza fare neppure troppo mistero della genesi «economico-finanziaria» di una siffatta scelta. Poi perché mai dovrebbe «collaborare» Facebook? La pagina del non identificato Postiglione Marco (magari non è neppure un fake) sarà stata cliccata di più proprio per le offese che recava al candidato alle elezioni comunali e ad ogni click il provider amplia il proprio profitto!

Come si esce da questa grave situazione: rendersene conto è già importante. Se le procure incominciano a comprendere l'allarme sociale che l'illecito in rete determina siamo già a buon punto; sono stati proposti pool o strutture simili per varie tipologie di reati; oggi c'è urgenza di magistrati specializzati in materia di Internet, perché il mezzo ha preso il sopravvento sul contenuto: un pm che sappia tutto sulla diffamazione non basta quando lo strumento è la rete.

Poi c'è il grande tema delle responsabilità politiche globali e nazionali: se non si costringono gli operatori a fare i conti con un territorio specifico, il suo diritto, le sue tasse da pagare, resistendo alla clamorosa offensiva lobbistica che questi compiono, tutto è vano. C'è una differenza rispetto al passato: il potere pubblico non ha più il

pallino in mano: non occorre attendere il futuro; già oggi una Procura deve arrendersi all'impossibilità di intervento e ben presto i governi capiranno che basta un click per creare loro un'opposizione interna ed internazionale.


IL MATTINO

L'addio che spacca i 5 Stelle

I due Napoli di Sarri e De Laurentiis

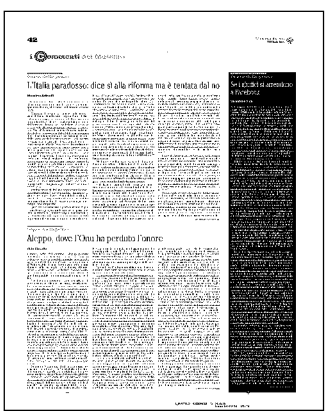
Bankitalia al governo «Crescita, stime alte»

La rapina milionaria alla sexy star

Se i giudici si arredano a Facebook

Perché si può indagare sulla terrante

idealista disegna dove vuol vivere


L'Italia paradosso: dice sì alla riforma ma è tentata dal no

Aleppo, dove l'Onu ha perduto l'onore

Il Sole 24 ORE

Data 10-10-2016
Pagina 22
Foglio 1

Il Ddl al Senato. Tutele estese anche agli adulti

Al Garante della privacy il potere di cancellare i post lesivi entro 24 ore

Potrebbe presto essere legge il Ddl per contrastare e prevenire il bullismo e il cyberbullismo: già approvato dal Senato e dalla Camera, il testo è ora a Palazzo Madama, in attesa di iniziare la terza lettura.

Il Ddl ha l'intento di rafforzare le funzioni del Garante per la privacy, investito del compito di oscurare entro 24 ore dal momento in cui riceve l'istanza i contenuti pubblicati nel web, come video e fotografie, ritenuti illeciti. L'intervento in realtà è articolato in due fasi. In prima battuta l'interessato dovrà contattare direttamente il social network, il gestore di messaggeria istantanea (ad esempio WhatsApp) o il sito internet. Soltanto in caso di mancata rimozione, sarà chiamato a provvedere tempestivamente il Garante.

La tutela, originariamente prevista soltanto per i minorenni, nell'ultima versione licenziata dalla Camera è stata estesa anche ai maggiorenni, sollevando non poche reazioni contrarie. La riforma, encomiabile negli obiettivi, rischia infatti di diventare l'ennesima presa di posizione su un problema che richiede, invece, soluzioni pratiche. Questo perché è difficile immaginare che il Garante della privacy possa intervenire operativamente in tutti i casi segnalati, anche dagli adulti. Il termine di 24 ore sembra essere soltanto indicativo e destinato a non reggere ai primi test pratici.

Le nuove norme rafforzano anche il ruolo dei social network e dei gestori dei siti in generale che dovrebbero dotarsi di specifiche procedure per ricevere le istanze da parte degli utenti.

L'estensione del meccanismo anche ai maggiorenni rischia di portare a ripetere quel che è accaduto in tema di diritto all'oblio. A distanza di oltre due anni dalla sentenza della Corte di giustizia europea che ha sancito il diritto degli utenti ad essere dimenticati dalla rete (pronuncia del 13 maggio 2014 nella causa C-131/12), i provider si sono dimostrati scarsamente collaborativi, rimettendo di fatto la rimozione dei contenuti all'iniziativa privata (si veda Il Sole 24 Ore dell'11 gennaio scorso).

Le nuove norme introducono inoltre una definizione di cyberbullismo, punito con la reclusione fino a sei anni, prevedendo un'estensione del reato di stalking che assorbirebbe anche le fattispecie di sostituzione di persona e trattamento illecito dei dati personali.

Il Ddl merita di essere sottolineato per almeno tre buone ragioni. In primo luogo introduce la figura del referente scolastico, che dovrà essere scelto in ogni istituto tra i docenti e che avrà il compito di organizzare iniziative di prevenzione e contrasto al bullismo e al cyberbullismo. Inoltre, sono previsti stanziamenti per finanziare progetti e azioni di contrasto al fenomeno. Infine, le nuove norme prevedono anche l'elaborazione di piani programmatici con i servizi sociali territoriali volti a sostenere i minori vittime di bullismo nonché a rieducare gli autori dei fatti illeciti. Tutte strategie che si muovono nella direzione della prevenzione e presuppongono una formazione specifica sui temi della privacy e del diritto dell'informatica.

La questione che resta centrale sarà quella dell'attuazione della riforma, che è soprattutto un problema di mezzi e di personale adeguatamente formato.

IN ESCLUSIVA PER GLI ABBONATI

I documenti citati in questa pagina
www.quotidianodiritto.ilsole24ore.com


Cyberbulli minorenni, pagano scuole e famiglie

Al Garante della privacy il potere di cancellare i post lesivi entro 24 ore

INVESTIRE IN FILATELIA

IL DUBBIO

Data 18-10-2016
Pagina 10
Foglio 1 / 2

«Il diritto all'oblio? Sul web è una chimera»

PARLA IL DOCENTE DELLA CATTOLICA DI MILANO RUBEN RAZZANTE, ESPERTO DI DIRITTO DELL'INFORMAZIONE

GIOVANNI M. JACOBAZZI

La triste storia di Tiziana Cantone, la ragazza costretta al suicidio il mese scorso dopo che un video hard girato con il suo fidanzato era diventato virale sui social, ha messo in evidenza come sia estremamente difficile oggi, nel mondo globalizzato dei media e della comunicazione, garantire la tutela della privacy. La povera Tiziana, per sfuggire alla gogna del web era stata costretta a cambiare nome e città. Ma non è stato sufficiente. E soprattutto, l'essersi rivolta all'Autorità giudiziaria per chiedere giustizia non è bastato: il video hard è rimasto al suo posto e con lui anche i commenti beceri di decine di migliaia di persone.

In materia di "diritto all'oblio", uno dei massimi esperti italiani è Ruben Razzante, professore di Diritto europeo dell'informazione e di Diritto della comunicazione per le imprese e i media presso l'Università Cattolica di Milano. A Razzante *Il Dubbio* ha chiesto di illustrare l'evoluzione della dottrina in materia di privacy e diritto di cronaca: venerdì prossimo 21 ottobre peraltro verrà presentata a Milano a Palazzo Cusani la settima edizione del suo *Manuale di diritto dell'informazione e della comunicazione: innovazione giuridica della Rete e deontologia giornalistica*. Il testo vede la luce a pochi mesi dall'emanazione del nuovo Testo Unico della deontologia giornalistica ed è in concomitanza con l'uscita del nuovo Regolamento europeo sulla privacy, destinato a cambiare la disciplina del trattamento dei dati personali in tutta Europa.

Professore, parliamo di processi mediatici. Un problema di cui si discute da anni ma che non sembra destinato ad essere risolto.

Il processo mediatico è diventato, di fatto, una anticipazione della pena. Questa grave stortura, a mio avviso, nasce per un duplice motivo. Da un lato, l'estrema lunghezza del processo che mal si concilia con i tempi rapidi della comunicazione. Da l'altro, la tendenza dei giornalisti a sostituirsi agli organi preposti ad esercitare la funzione giurisdizionale. Il combinato di questi due fattori determina ricostruzioni fattuali completamente distorte. A ciò si aggiunga il numero veramente elevato di programmi in cui si discute di fatti reato senza conoscere il ben che minimo atto d'indagine. Sono questi dei "salotti dell'ovvio" molto pericolosi perché condizionano fortemente l'opinione pubblica. E, nel caso di processi in Corte d'Assise, con la presenza di giudici popolari non particolarmente strutturati a reggere una tale pressione mediatica, ciò può avere effetti devastanti.

Qual è il motivo di questa degenerazione comunicativa?

Il discorso è molto complesso. E riguarda il mondo dell'informazione nella sua totalità. Ma partiamo dalla carta stampata: il voyeurismo giudiziario per lungo tempo ha pagato in fatto di vendite di copie dei giornali. Fino a poco tempo fa, senza fare nomi, i quotidiani che avevano impostato la loro linea editoriale sull'antiberlusconismo più sfrenato, pubblicando pagine e pagine di intercettazioni telefoniche che lo riguardavano, avevano grande successo nelle edicole.

Finito Berlusconi quegli stessi giornali hanno conosciuto un calo di vendite: la stampa italiana ha bisogno di un nemico?

C'è uno stretto legame fra una democrazia matura ed una stampa matura. In Italia, rispetto ad altri paesi occidentali, siamo molto indietro. Il confronto dialettico si svolge sempre con toni inutilmente esasperati. Le ho citato prima la dinamica fra berlusconiani e antiberlusconiani. Diciamo che quel ventennio ha condizionato fortemente non solo la vita politica italiana ma anche l'informazione. Senza più Berlusconi il sistema è andato in crisi.

Che futuro vede per la stampa italiana?

Fra i miei studenti, fascia d'età 19-24 anni, nessuno la mattina prima di venire a lezione compra più un giornale di carta. Ma possiamo alzare tranquillamente la soglia d'età fino ai 30 anni. I loro canali d'informazione sono diversi. Social, condivisione di notizie, blog. Neppure i siti informativi. Anzi, sono pochi quelli che guardano pure i telegiornali. Ma in questo c'è anche l'aspetto positivo dovuto alla possibilità di interagire con le notizie.

Non si preannuncia un futuro roseo per i giornali.

I giornali di carta potranno salvarsi solo se tratteranno approfondimenti specifici. Con notizie non reperibili in rete. O, nel caso dei quotidiani locali, se approfondiranno temi come la cronaca cittadina. I quotidiani generalisti sono destinati a finire se non si rinnoveranno presto. Si può prevedere che ci siano diversi accorpamenti di testate nel prossimo futuro. E molti quotidiani si trasformeranno in settimanali.

Quindi il condizionamento dei giornali sull'opinione pubblica è ormail un ricordo?

Sicuramente. Ormai le persone hanno altri mezzi per formare la loro opinione su determinati temi rispetto all'editoriale del direttore.

La rete però può essere fuorviante: in molti si lasciano convince dell'esistenza delle scie chimiche e di chip sotto cute per controllare la popolazione.

La rete ha grandi potenzialità che non c'è bisogno di ricordare. Ma i blog sono un problema serio. La diffusione indiscriminata di notizie è deleteria. Sarebbe opportuno, ad esempio, mettere un "bollino" alla fine dell'articolo. Per indicare che è stato scritto da un giornalista, riportando pure il numero della tessera di iscrizione all'Ordine. Ciò per differenziare chi scrive per puro diletto perché prendeva otto in italiano e chi deve rispettare la deontologia professionale. E poi fare un patto con i motori di ricerca per la tutela dei contenuti giornalistici in rete, evitando quindi contenuti indifferenziati.

Il diritto all'oblio non sembra facilmente realizzabile. A che punto siamo?

Su questo tema c'è molta confusione. Il diritto all'oblio non è il diritto al "colpo di spugna" con cui cancellare le notizie scomode. Sarebbe come andare nell'archivio di un quotidiano e strappare le pagine che non ci piacciono. Se corrisponde ad un criterio di verità e di interesse pubblico, la notizia non può essere cancellata. Quello che si può fare è chiedere la deindicizzazione dell'url della notizia dai motori di ricerca. Google ha predisposto un apposito modulo. Se Google non risponde ci si può rivolgere ai giudici o al Garante della Privacy. Ma su questo aspetto bisogna fare una precisione. In caso di politici, personaggi pubblici, ciò di fatto è impossibile. Faccio un esempio: se un amministratore pubblico è stato coinvolto in procedimento penale e poi è stato assolto, anche se chiedesse la deindicizzazione di tutti gli articoli sulla sua vicenda processuale si vedrebbe opporre un rifiuto da Google. L'interesse pubblico alla conoscenza della notizia viene prima rispetto agli effetti della reputazione che questa notizia può avere sul diretto interessato.

Quello che lei dice è ignoto alla stragrande maggioranza degli uteni del web.

L'unica speranza è il tempo. Nel misterioso ed imperscrutabile algoritmo di Google il trascorrere del tempo è un fattore importante. Riguardo l'amministratore pubblico assolto, se questi si ritirasse a vita privata non facendo più parlare di sé, è probabile che la notizia verrebbe deindicizzata.

Quindi, acquisito che una notizia è per sempre, cosa si può fare?

Bisogna essere molto accorti a cosa condividiamo sulla rete. Consapevoli che non potrà mai essere cancellato. L'unica soluzione è l'autotutela. Nessuna legge ci garantisce l'oblio dalla rete. Non creiamo false aspettative.

«AL MASSIMO SI PUÒ OTTENERE CHE GOOGLE SMETTA DI INDICIZZARE UNA CERTA PAGINA. MA LA PROFESSIONALITÀ DEI BLOGGER È ORMAI UN PROBLEMA: ANDREBBE IMPOSTO UN BOLLINO PER DISTINGUERE I VERI GIORNALISTI»


SOCIETÀ

PARLA IL DOCENTE DELLA CATTOLICA DI MILANO RUBEN RAZZANTE, ESPERTO DI DIRITTO DELL'INFORMAZIONE

«Il diritto all'oblio? Sul web è una chimera»

LA STAMPA

Data 21-10-2016
Pagina 15
Foglio 1 / 3

Un americano su due è schedato grazie al riconoscimento facciale

In Usa il primo studio sul software che identifica le persone da una foto Serve per catturare criminali, ma a oggi non ci sono regole e limiti

il caso

CAROLA FREDIANI

Immaginate un classico confronto all'americana, con un sospettato da identificare in una fila di persone, più o meno simili, in piedi. E immaginate che la fila da cui scegliere si allunghi sempre di più fino a includere 117 milioni di adulti statunitensi. E che ad abbinare uno di questi cittadini ai volti di indiziati, ripresi da qualche videocamera sparsa per la città, siano degli algoritmi utilizzati dalle polizie di una trentina di Stati come fossero un semplice motore di ricerca. Si immette l'immagine del presunto criminale e si cerca un possibile collegamento con una foto tratta dalle banche dati delle patenti di guida o delle carte d'identità. Ebbene, non c'è più bisogno di immaginare: negli Usa è già realtà.

Lo studio

Un americano adulto su due ha avuto le sue foto sottoposte a questo genere di ricerche. A dirlo è il primo studio onnicomprensivo sull'utilizzo delle tecnologie di riconoscimento facciale svolto negli Stati Uniti, a firma di un autorevole istituto di studi su privacy e tecnologia: «The Center on Privacy & Technology» della Georgetown University. La tesi della ricerca è che l'adozione del riconoscimento facciale sia inevitabile, anche ai fini di sicurezza, e non possa o debba essere fermato. E tuttavia che allo stato attuale sia del tutto deregolamentato e per nulla monitorato in termini di uniformità di procedure, limiti di applicazione, efficacia. La politica, quindi, dovrebbe intervenire in modo da gestirlo per tempo. Diversamente, il rischio è che si crei una società del «confronto all'americana perpetuo», come alluso nel titolo della ricerca: «The Perpetual Lineup».

Senza regole

Tra le criticità, dice lo studio, c'è il modo in cui sono usati questi sistemi. Un conto è fare una ricerca per identificare qualcuno che è stato fermato o arrestato. Un altro paio di maniche è avere l'immagine di un sospetto presa da una videocamera e cercarla in un database composto dalle patenti di comuni cittadini o da immagini riprese da videocamere mentre sono per strada. Nel primo caso è una ricerca mirata e al contempo pubblica, palese. Nel secondo è invece tanto generica quanto invisibile. Oggi, ogni dipartimento o agenzia locale americana fa quello che vuole.

Andando a pescare dagli archivi delle patenti però l'Fbi sta costruendo una risorsa di dati biometrici che include cittadini rispettosi della legge. Mentre storicamente le impronte digitali e il Dna sono stati raccolti in relazione ad arresti o indagini criminali. Tutto ciò, dice lo studio, non ha precedenti ed è problematico. Così come lo è l'impiego di video in tempo reale registrati dalle telecamere di sorveglianza: sono almeno cinque i dipartimenti di polizia che utilizzano funzioni di riconoscimento facciale di questo tipo su videocamere in strada. Inoltre, di 52 agenzie che adottano in generale questa tecnologia, solo una proibisce espressamente il suo utilizzo per monitorare individui coinvolti in attività politiche o religiose. Il rischio di utilizzi impropri, discriminatori ad esempio verso afroamericani o minoranze, è alto.

L'affidabilità del sistema

Lo studio mette poi sul piatto il tema cruciale della verifica del funzionamento di tali sistemi. Solo due agenzie hanno subordinato l'acquisto a test di efficacia. E una delle maggiori aziende del settore, FaceFirst, che sostiene di avere un tasso di accuratezza del 95 per cento, declina ogni responsabilità nel caso in cui non raggiunga la soglia prevista dai contratti con le agenzie locali. A ciò, va aggiunta l'assenza di controlli e meccanismi per rilevare eventuali abusi: solo nove agenzie su 52 registrano le ricerche effettuate nei database dai loro agenti.

117 milioni
È il numero di adulti americani che attualmente sono stati schedati attraverso sistemi di riconoscimento facciali

52 agenzie
Sono oltre cinquanta le agenzie di sicurezza americane che utilizzano software di riconoscimento facciale nel loro lavoro

98 per cento
Solo una delle 52 agenzie vieta espressamente l'utilizzo del software per monitorare individui coinvolti in attività politiche o religiose

Spionaggio

In vendita sul web i segreti dell'Nsa

Il New York Times riporta la notizia che documenti top secret dell'Nsa sarebbero finiti in vendita su internet. Si tratta del dossier trafugato da Harold Martin III, veterano della Marina arrestato in agosto. Il materiale fa impallidire per mole quelli di Snowden.

Gli usi e gli abusi

Sicurezza

L'Italia lancia un bando "Strumento utile per l'antiterrorismo"

56 milioni
A novembre il ministero dell'Interno italiano ha indetto una gara per sistemi di videosorveglianza

L'industria del riconoscimento facciale è spinta anche dalle richieste di sicurezza degli Stati. Tra gli utilizzi più diffusi finora c'è la ricerca del volto di qualcuno fermato a una frontiera, dopo averlo fotografato con lo smartphone, su un database di sospettati o criminali.
Lo fa ad esempio la Turchia. Più complessa, ma molto ambita dalle forze di sicurezza, la ricerca fatta su immagini registrate da telecamere a circuito chiuso o riprese in tempo reale da videocamere di sorveglianza.
Ambizione espressa anche del governo italiano che con il ministro dell'Interno Angelino Alfano aveva annunciato un potenziamento del sistema di sicurezza del Paese che includeva anche questo genere di tecnologia.
Lo scorso novembre è stata indetta una gara pubblica da 56 milioni di euro per la fornitura di sistemi di videosorveglianza (per edifici pubblici e per il territorio) con funzioni di analisi video in tempo reale e riconoscimento facciale. **[CAR. FRE.]**

Identificazione

In mano a uno stalker può diventare un'arma pericolosa

70 per cento
I creatori di Find Face dichiarano che la loro app è in grado di riconoscere una persona al 70%

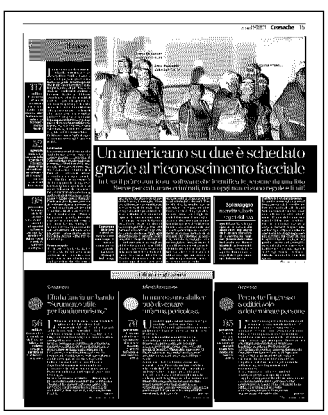
Una delle applicazioni commerciali più inquietanti del riconoscimento facciale è quella già adottata da alcune piattaforme di appuntamenti, come la russa FindFace.
Quest'ultima utilizza una tecnologia avanzata per abbinare foto scattate a sconosciuti per strada, per esempio attraverso lo smartphone, con i volti dei profili di iscritti a Vkontakte, una sorta di Facebook russo. Secondo i suoi creatori avrebbe un tasso di successo del 70 per cento.
Alcuni utenti che lo hanno testato sono riusciti a identificare donne fotografate in altri contesti. È chiaro che il potenziale per stalking e abusi di ogni tipo è altissimo.
Tutt'altro utilizzo è invece quello pensato dalla app di dating Heystax, che lavora sullo studio delle espressioni facciali dei suoi utenti mentre sono impegnati in una videochiamata con un potenziale partner. La pretesa qui è di valutare la compatibilità emozionale della coppia. **[CAR. FRE.]**

Accesso

Permette l'ingresso a edifici solo a determinate persone

95 per cento
L'azienda italiana Eurotech dichiara che il suo software riconosce una persona al 95%

L'efficacia maggiore delle tecnologie di riconoscimento facciale avviene nei cosiddetti contesti cooperativi, laddove cioè le persone si fermano e si fanno volutamente inquadrare da videocamere. Un utilizzo che funziona per dare l'accesso a luoghi riservati: per esempio edifici o cantieri con esigenze particolari di sicurezza. L'azienda israeliana Fst Biometrics pubblicizza da qualche anno un sistema che dovrebbe funzionare da pass di ingresso negli edifici, al posto di chiavi, badge e password. Basta dare inizialmente una propria foto al sistema e poi, al momento dell'accesso, farsi inquadrare dalla videocamera.
Tra le aziende in Italia c'è Eurotech a lavorare proprio su questo genere di applicazioni, promettendo un tasso medio di identificazione del 95 per cento. Può monitorare il transito di un visitatore in un edificio o abbinare il suo volto a un documento precedentemente registrato per identificarlo. [CAR. FRE.]


Un americano su due è schedato grazie al riconoscimento facciale

Il Messaggero

Data 22-10-2016
Pagina 1
Foglio 1

Web in tilt per ore Hacker scatenati Usa sotto attacco

Flavio Pompetti

Due ore di blocco degli accessi e di oscuramento per i siti e i servizi più popolari del web. *A pag. 12*

America sotto attacco Per due ore il web oscurato dagli hacker

▶Bloccati agli utenti Usa i siti di Cnn e Twitter, stop a Netflix e Playstation. E i cinesi entrano nel software di una portaerei

IL CONFLITTO

NEW YORK Due ore di blocco totale degli accessi, due ore di oscuramento per i siti e i servizi più popolari del web. Hacker anonimi hanno attaccato ieri di prima mattina il server americano Dyn, una sorta di centralino elettronico che collega ogni utente che digita un indirizzo di internet sul suo computer, alla pagina richiesta. Gli abitanti della costa atlantica negli Usa al risveglio hanno trovato la porta chiusa quando hanno provato a leggere le notizie della Cnn e del Financial Times, del New York Times, del britannico The Guardian e della rivista Time. Niente acquisti su Amazon eBay ed Etsy, niente musica su Spotify; spento il proiettore di Netflix, spenta anche la Playstation.

IL SEGNALE "DDOS"

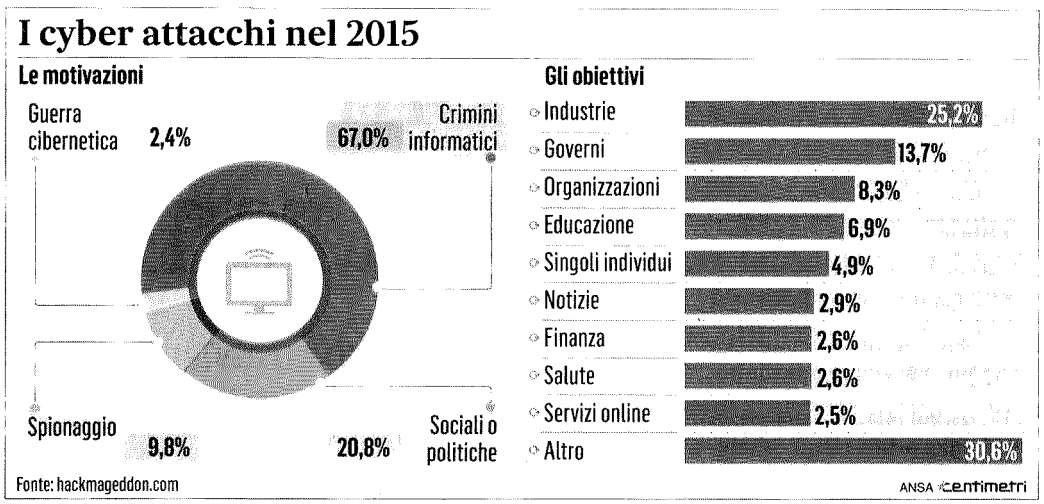
I pirati stavano bombardando Dyn con una valanga di richieste di accesso fittizie, che investivano a ondate il server fino a mandarlo in tilt. Per lunghi periodi e per la durata di due ore, le pagine più popolari del web, frequentate da milioni di utenti americani, sono rimaste chiuse: i visitatori ricevevano un segnale di DDoS (Distributed Denial of Service: rifiuto di servizio) che ha generato equivoci e numerose proteste. Non ci sono prove che puntino verso i responsabili della violazione, ma la tenue traccia che la lega ad attacchi precedenti è tale da destare la massima preoccupazione. La tecnica usata è simile a quella messa in atto lo scorso settembre contro il giornalista investigativo Brian Kreb, il quale aveva appena collaborato con l'Fbi per l'identificazione e l'arresto di due israeliani, due sicari di Internet che lanciavano attacchi a pagamento. La Dyn ha collaborato con Kreb per difendere il suo sito dagli attacchi, e il sabotaggio di ieri ai danni della Dyn potrebbe essere un atto di ritorsione da parte degli hacker infastiditi dagli arresti.

Quello che spaventa in questa ricostruzione è la totale sproporzione che potrebbe esserci tra il livello dei pirati e la portata dei danni che sono in grado di provocare. Una sproporzione che in questi giorni è sotto gli occhi di tutti con l'influenza indebita che lo spionaggio cibernetico russo sta avendo sul processo elettorale americano. La Homeland Security ha aperto un'indagine sull'accaduto. Un altro esempio della debolezza degli Usa di fronte alla pirateria elettronica si è avuto ieri con la rivelazione fatta al Financial Times dai tecnici della FireEye, un'azienda statunitense specializzata in sicurezza informatica. Questi ultimi hanno detto che lo scorso 11 di luglio hacker, probabilmente cinesi, sono riusciti a infiltrare con il malware Enfal il computer di un funzionario straniero a bordo della portaerei Ronald Regan, in pattuglia nel Mare cinese meridionale. L'obiettivo era carpire i segreti della strategia della Marina americana nella regione, e non è chiaro se il tentativo è riuscito.

LA SENTENZA

La beffa è che l'infiltrazione è avvenuta il giorno prima del pronunciamento del tribunale dell'Aia, che ha poi condannato le pretese territoriali di Pechino nel mare Cinese meridionale, motivo dell'intrusione della portaerei americana nell'area. La sentenza era stata richiesta dal presidente filippino Benigno Aquino, ma dopo le elezioni estive il suo successore Rodrigo Duterte ha insultato a più riprese gli americani e il loro presidente Obama, fino a rinnegare l'alleanza che legava le Filippine a Washington.

Flavio Pompetti



CORRIERE DELLA SERA

Data 23-10-2016
Pagina 10
Foglio 1

Gli hacker nel frigorifero

Il cyber attacco che venerdì ha paralizzato Internet negli Usa è partito dalle case «intelligenti» dei cittadini (a loro insaputa) Wikileaks rivendica, allarme globale

L'attacco è arrivato da videoregistratori, frigoriferi, telecamere di sicurezza, router e sistemi per il controllo dei neonati. Quella che sembra la trama di un film di fantascienza, neanche dei più raffinati, è invece il racconto degli esperti sull'attacco informatico che ha bloccato il Web americano per tutta la giornata di venerdì. Un cyber-attacco che bloccando i server della Dyn, azienda del New Hampshire che svolge il compito di indirizzare il traffico Web, di fatto ha reso inaccessibili a milioni di utenti centinaia di siti. Da quelli di giornali come New *York Times* e *Financial Times*, a quelli di servizi a dir poco popolari: Twitter, Netflix, Spotify, AirBnb e molti altri. Alla base, come esercito, ci sarebbe l'Internet of Things, i miliardi di oggetti comuni collegati al Web.

I generali che hanno condotto l'offensiva sono ancora oggetto di indagine: si parla di hacker russi o cinesi, di «vandali della Rete», ma anche di seguaci di Julian Assange, come lasciava intendere ieri un tweet di Wikileaks: «Chiediamo a tutti i sostenitori di smettere di attaccare i siti internet Usa». Una sorta di rivendicazione indiretta. In ogni caso negli Usa, alla vigilia delle elezioni, l'allarme è molto alto.

Cosa è successo

I server della Dyn gestiscono parte del «Domain Name System» della rete americana, ossia si occupano di tradurre in numeri comprensibili ai computer quegli indirizzi che digitiamo nei browser, come «Corriere.it». Dalle ore 7 del mattino locali sono iniziati i primi problemi che, in diverse ondate, hanno portato al blackout parziale della Rete americana, che da una costa si è spostato sull'altra. Secondo quanto emerso nella tarda serata di venerdì, l'attacco di tipo Ddos — Distributed Denial of Service — sarebbe partito da migliaia di oggetti «smart», che dalle case di cittadini all'oscuro hanno intasato i server dell'azienda di «false richieste» al punto di zittirli del tutto. Si tratta di oggetti sempre più diffusi — secondo gli analisti di Gartner oggi se ne contano 7 miliardi nel mondo, nel 2020 saranno quasi 30 — e rappresentano forse il più grande problema di sicurezza informatica del momento, perché vulnerabili ad attacchi esterni. Quanto successo poche ore fa negli Stati Uniti sarebbe stato causato da dispositivi resi «zombie», ovvero pilotati a distanza, da un software «cattivo» chiamato «Mirai», una sorta di virus che negli ultimi tempi avrebbe infettato centinaia di migliaia di registratori digitali, telecamere, sensori di vario genere e altri oggetti connessi ala Rete.

I sospetti

Queste tipologie di attacchi condotti attraverso «smart devices», secondo il colosso americano della Rete Verisign, sono aumentati del 75% negli ultimi mesi rispetto all'anno precedente. Diventando sempre più massici e sofisticati. Secondo il blogger Bruce Schneier, un esperto di sicurezza citato tra gli altri dal *New York Times*, sembra che dietro ci sia una specie di disegno, come se qualcuno stesse mettendo alla prova le difese delle aziende che gestiscono pezzi del traffico di Internet. Potrebbe trattarsi di Paesi «nemici» come Russia e Cina, con cui gli Usa avrebbero già da tempo ingaggiato una guerra informatica neanche troppo sotterranea — il vicepresidente Biden, a inizio mese, aveva avvertito della capacità americana di rispondere alle cyber provocazioni —, oppure di gruppi di hacker più o meno isolati. L'*Associated Press* racconta della rivendicazione via Twitter da parte di un collettivo «ombra» New World Hackers: avrebbero scatenato «zombie» capaci di generare traffico fasullo sui server della Dyn per 1,2 Terabit al secondo.

Il voto online

Se è troppo presto per poter trarre conclusioni, non lo è per preoccuparsi in vista del voto per le Presidenziali del 8 novembre. Sono infatti 31 gli Stati americani che permettono il voto online per i militari e i civili che si trovano Oltreoceano, con in più l'Alaska. Secondo l'Election Assistance Commission, un'agenzia indipendente creata nel 2002 per agevolare la partecipazione degli americani alle elezioni, un attacco Ddos potrebbe fortemente influire sul voto elettronico. Arrivando a determinare, per esempio, l'esito del ballottaggio negli «swing states», gli stati più in bilico tra Clinton e Trump.

Federico Cella
@VitaDigitale

«Mirai» in azione
Il nome del virus che di recente avrebbe infettato un'infinità di oggetti connessi al Web


Gli hacker nel frigorifero

«Spiare WhatsApp e Telegram è un gioco da ragazzi»

Il Messaggero

Data 23-10-2016
Pagina 12
Foglio 1

Assalti hacker, Assange "ordina" lo stop Pc e baby monitor: così hanno colpito

IL CASO

NEW YORK «Ora basta, avete raggiunto il vostro scopo ma è ora di smetterla». Il Twitter di Julian Assange, alla fine di una giornata di caos e di servizio a singhiozzo per centinaia dei siti web più popolari del mondo, sembra un'assunzione di paternità per il ciber attacco che ha paralizzato venerdì il traffico Internet sulla costa orientale degli Usa. Ma quanto è credibile l'appello del recluso dell'ambasciata ecuadoriana a Londra?

LE RIVENDICAZIONI

Lo stesso atto di pirateria è stato rivendicato da hackers individuali e da gruppi organizzati, e l'FBI che sta indagando quanto è accaduto non ha ancora escluso che dietri le varie sigle si nasconda un intero apparato di intelligence nazionale: quello russo ad esempio, o magari quello cinese. Per tre volte durante l'arco della giornata chi cercava di accedere alle pagine di Twitter e di Spotify, di Netflix e di eBay, ha trovato la strada sbarrata. Il vigile elettronico che avrebbe dovuto smistare le richieste era paralizzato da una valanga di domande di accesso fasulle, fabbricate con il solo scopo di intasare il sistema e bloccarlo.

Uno scherzo che ha messo in ginocchio decine di aziende che operano su Internet, ha umiliato il controllore del traffico: l'americana Dyn del New Hampshire, ed è costata milioni di dollari in pubblicità perduta per gli inserzionisti. Gli hackers hanno usato come arma l'Internet delle Cose, la capacità cioè che hanno oggetti diversi che sono entrati nelle nostre case e fanno parte delle nostre abitudini, di comunicare tra loro. Nella rete circa un mese fa è apparso Mirai, un virus destinato a raggiungere router e baby monitor, macchine fotografiche e stampanti.

Tutto quanto collegato al computer casalingo, specialmente se dotato di una password molto semplice da identificare, o addirittura mai personalizzata rispetto a quella pre-installata dalle case produttrici. Mirai è stato fatto entrare in azione venerdì da qualcuno che ne aveva le chiavi, e che ha chiesto a questo esercito (nel mondo ci sono dai 10 ai 15 miliardi di oggetti che appartengono all'Internet delle Cose) di entrare in funzione, mandando una richiesta di accesso alla Dyn, la quale smista le richieste di accesso per il 6% delle aziende che fanno parte della lista Fortune 500, le 500 aziende più ricche d'America.

NON SOLO WIKILEAKS

Oltre che da Wikileaks la paternità dell'attacco è stata rivendicata da un gruppo che si identifica come New World Hackers, e che dice di aver scatenato nei confronti della Dyn un volume di 1,2 terabites (1.200 miliardi di bites) per secondo. Dicono di essere un collettivo di trenta persone sparse nel mondo: dalla Russia all'India e alla Cina, e che dieci di loro hanno partecipato all'attacco, dopo aver in passato boicottato i network della ESPN, della BBC e dell'Isis, sia in Siria che in Iraq.

Da Londra un'altra rivendicazione è stata fatta dal gruppo omologo Ownz. L'FBI e la Homeland Security americana stanno investigando, e finora non hanno annunciato nessuno sviluppo delle indagini. L'episodio, per quanto impressionante per grandezza ed efficacia, non è comunque del tutto nuovo. Il mese scorso un rapporto pubblicato dall'esperto per la sicurezza digitale Bruce Schneider, dal titolo «Qualcuno sta imparando come paralizzare l'Internet» ha denunciato la frequenza con la quale molti dei siti di maggiore traffico abbiano sperimentato in tempi recenti lo stesso 'Rifiuto di Servizio' che venerdì è apparso a più riprese come risposta alla richiesta di accesso delle pagine colpite dall'attacco. Gli hackers sono riusciti a diffondere Mirai approfittando di computer non protetti e di facile accesso.

Il virus non ha compromesso nessuna delle funzioni, e per questo è rimasto ospite delle apparecchiature nelle quali si era inserito senza destare allarme, fino al comando di attivazione. Chi ne è stato contagiato può rimuoverlo cambiando la password dell'oggetto elettronico, ma non può cancellarlo: dopo un po' di tempo riappare, silenzioso e pronto ad entrare nuovamente in azione.

Flavio Pompetti

OGGETTI DIVERSI INFETTATI DAL VIRUS «MIRAI» INCHIESTA DELL'FBI DOPO L'ATTACCO AGLI STATI UNITI

CORRIERE DELLA SERA

Data 23-10-2016
Pagina 10
Foglio 1

«Spiare WhatsApp e Telegram è un gioco da ragazzi»

Una società milanese trova e denuncia una falla nel sistema: abbiamo assistito alla prova

L'intervento

di **Gianfranco Giardina**

L'annuncio è tale da far tremare i polsi: violare un account WhatsApp o Telegram sarebbe un gioco da ragazzi. La vulnerabilità, portata alla luce da InTheCyber, società milanese specializzata nella sicurezza offensiva e difensiva informatica, si concretizza grazie alla facilità di accesso indebito delle segreterie telefoniche di alcuni gestori e alle procedure di autenticazione dei sistemi di messaggistica, incautamente basati su messaggi telefonici vocali. La semplice procedura necessaria per la violazione è stata mostrata in anteprima al *Corriere della Sera* e verrà presentata domani, durante la settima Conferenza sulla Cyber Warfare a Milano.

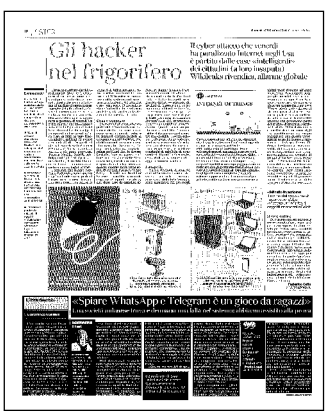
Si tratta di una falla di sicurezza importante (secondo i tecnici di InTheCyber riguarderebbe a diverso titolo circa 32 milioni di Sim italiane), anche in considerazione del fatto che per sfruttarla non serve alcun basista all'interno delle telco (gli operatori di telecomunicazione), nessuna apparecchiatura sofisticata e bastano competenze tecniche minime.

Malintenzionati o anche solo curiosi possono di fatto avere libero accesso al testo integrale delle chat di Telegram o ai gruppi di WhatsApp, conoscendo solo il numero di telefono della vittima e niente più. Il problema, secondo i tecnici di InTheCyber, al momento è fortemente sottovalutato: «WhatsApp, da noi informata della vulnerabilità, si è detta semplicemente "non interessata al problema" perché, secondo la società, la responsabilità sarebbe delle telco. Telegram invece non ha risposto alla nostra segnalazione, come anche i gestori telefonici che abbiamo contattato». Una situazione che contrasta con la scritta che campeggia sul sito di WhatsApp: «La privacy e la sicurezza sono nel nostro Dna».

«Questa vulnerabilità può essere chiusa facilmente con la collaborazione delle telco e dei fornitori di servizi — ci spiega Paolo Lezzi, Ceo e fondatore di InTheCyber — ma è solo la dimostrazione dello stato non ottimale in cui versa la sicurezza dei sistemi informatici e digitali». La diffusione sempre più capillare dell'Internet degli Oggetti e della iper-connessione richiede una maggiore consapevolezza da parte degli utenti «ma soprattutto ci vorrebbero — prosegue Lezzi — obblighi e responsabilità chiare per chi progetta e gestisce i prodotti e i servizi connessi, sia a livello pubblico che privato».

Spesso si pensa che gli effetti di un attacco restino confinati alla sfera digitale e che possano comportare, come massimo rischio, la cancellazione dei dati; ma le conseguenze di un atteggiamento disattento sul fronte della cyber sicurezza possono finire per riguardare anche la sfera fisica. «Una vulnerabilità banale come questa da noi dimostrata può mettere a repentaglio la sicurezza delle persone, a cascata anche quella dell'ente o azienda per cui lavorano e, in caso di utilizzi estremamente malevoli, del Paese intero».

La notizia arriva nel giorno in cui il ministro dell'Interno Alfano ha comunicato che dall'inizio dell'anno sono stati censiti 626 cyber attacchi alle strutture critiche italiane. Qualcosa di più di un campanello di allarme.


Gli hacker nel frigorifero

«Spiare WhatsApp e Telegram è un gioco da ragazzi»

Il Messaggero

Data 24-10-2016
Pagina 14
Foglio 1

Asse 007-aziende e più fondi: la sfida italiana al cybercrime

▶Così si sta preparando il nostro Paese per difendersi in caso di blitz degli hacker

▶Test in corso per l'aggiornamento del piano per la protezione cibernetica

IL FOCUS

ROMA Non solo prevenire le minacce ed evitare i furti di dati riservati e sensibili a governi ed aziende, la cyber sicurezza è molto di più. E un esempio concreto di quanto possa essere importante impedire le intrusioni informatiche l'ha fatto meno di un mese fa Alessandro Pansa, direttore generale del Dis (Dipartimento per le informazioni della sicurezza) al forum Cybertech 2016: i risultati del test di hacking, realizzato su alcuni modelli di automobile Tesla, hanno mostrato vulnerabilità che, se sfruttate, avrebbero consentito ai potenziali aggressori di prendere il controllo dei freni dei veicoli. Così mentre i servizi segreti cercano alleanze con i privati, come il protocollo già firmato tra Dis e il gruppo Leonardo-Finmeccanica, una rete di sicurezza "partecipata" è già attiva: 500 docenti e 34 facoltà italiane collaborano con gli 007 sulla sicurezza informatica. Pansa, però, parla di minacce in aumento che non soltanto possono paralizzare il Paese e mettere a rischio la sicurezza nazionale, ma causare danni sul piano fisico anche in termini di feriti e, nel caso peggiore, di vittime. L'Italia deve ancora fare tanto, dice. La legge di stabilità 2016 ha previsto 150 milioni di euro per rafforzare la cyber security, intanto è arrivata la nomina di Diego Piacentini, presidente di Amazon, a commissario governativo per la digitalizzazione e l'innovazione, una scelta che rientra nella strategia nazionale per la sicurezza delle amministrazioni pubbliche.

IL PIANO

Le prove per testare la capacità di resistenza dei singoli Paesi e del sistema-web, sono in corso, l'Italia sta aggiornando il "Piano nazionale per la protezione cibernetica e la sicurezza informatica" in base alla direttiva Ue sulla network and information security, adottata il 6 luglio scorso dal parlamento europeo. Tra le ipotesi al vaglio del governo c'è la creazione di "un laboratorio" crato da Palazzo Chigi per testare i sistemi informatici prima del loro impiego nell'ambito di infrastrutture critiche, sia governative che private: da un lato la capacità di raccolta, analisi e conservazione dei dati, ormai in quantità immense (i big data), per individuare e disarticolare in anticipo la minaccia e, dall'altro, contare su nuove sensibilità dei provider nel sostenere gli attori pubblici nel loro sforzo di garantire la sicurezza.

LA NORMATIVA

La cyber sicurezza in Italia fa capo alla presidenza dl consiglio dei ministri, dopo le polemiche e i rinvii sulla nomina di Marco Carrai a super consulente del premier per i big data e la sicurezza informatica, oggi il coordinamento delle strutture interministeriali spetta a Carmine Masiello, consulente militare del premier. Il decreto del 2013 definisce tre diversi livelli di intervento: indirizzo politico e coordinamento strategico, supporto e raccordo tra gli enti competenti, gestione della crisi con un ruolo centrale del Dis e la creazione presso l'Ufficio del Consigliere militare, del Nucleo per la sicurezza cibernetica (Nsc), con funzioni di coordinamento delle varie componenti (ministeri, polizia postale a agenzia per l'Italia digitale, servizi di sicurezza) e di supporto per le attività del presidente del consiglio, per la preparazione e la prevenzione delle crisi. Il consigliere militare presiede anche il "Tavolo interministeriale di crisi cibernetica".

Valentina Errante

500
I docenti universitari che partecipano alla rete per la sicurezza.

34
Le facoltà universitarie che collaborano attivamente con gli 007.

ALLARME DI PANSA: IN AUMENTO LE MINACCE CHE POSSONO METTERE A RISCHIO LA SICUREZZA

Il Messaggero

Data 05-11-2016
Pagina 7
Foglio 1

L'intervista Antonello Soro

«La rete deve tutelare meglio l'utente sia più consapevole»

▶Il Garante: «Una volta inseriti nostre foto o dati diventa difficile averne il controllo»

▶«Se l'intervento dei gestori è tempestivo si può contenere il danno alle vittime»

Il diritto insegue il progresso tecnologico. Ecco il rebus di fronte al quale si trova, anche per la sollecitazione di clamorosi casi di cronaca, Antonello Soro, presidente dell'Autorità garante della protezione dei dati personali (o privacy). Che mette in guardia contro l'enormità dei pericoli. «La rete non è un mondo virtuale ma reale. È una dimensione della vita complicata e piena di insidie, di cui gli utenti devono essere consapevoli».

Si può essere involontari artefici della propria rovina, come la povera Tiziana Cantone suicida dopo la diffusione virale di video hard che lei stessa aveva inviato a contatti facebook?

«Certo, la Rete non è mai circoscritta. È un oceano nel quale una volta che abbiamo lanciato una nostra immagine o dato personale, difficilmente ne avremo il controllo».

È vero che in Rete tutto lascia traccia?

«Accidenti se è vero! Una conversazione in piazza può rimanere tra 5-6 persone, in rete è potenzialmente aperta a tutto il mondo».

Una sentenza civile a Napoli Nord ha stabilito che Facebook doveva rimuovere per tempo link e informazioni su Tiziana, ma ha escluso il controllo preventivo dei provider sui contenuti postati dagli utenti. Intanto in Germania la procura di Monaco ha indagato il fondatore di Facebook, Mark Zuckerberg, per la mancata eliminazione di post con minacce di morte e negazioni dell'Olocausto. Come ci si deve orientare in questo ginepraio?

«Si conferma la tendenza a responsabilizzare i gestori dei social network per tutelare in tempo chi in rete sia o presuma di essere vittima di contenuti lesivi e/o offensivi. A Napoli e a Monaco, si imputa a Facebook l'omessa rimozione. L'oscuramento dei contenuti non può seguire procedure troppo lunghe: l'intervento tempestivo contiene di molto il danno tecnologico permanente di una notizia messa in rete e poi moltiplicata in modo pulviscolare in tutto il mondo. Occorrono forme agili e immediate come quelle che si stanno disciplinando con la nuova legge in discussione in Parlamento sul cyber-bullismo. Nella stessa direzione va l'accordo di qualche mese fa tra i gestori di social network e la Commissione europea circa lo 'hate speech', l'istigazione all'odio, con interventi immediati, anche tramite filtri su certe espressioni. Bisogna armonizzare la tutela dei diritti off line con quella dei diritti on line. Vita fisica e digitale vanno trattate allo stesso modo, sulla base degli stessi obblighi e diritti che pretendiamo nella vita fisica in cui ci siamo abituati a rispettarci. Questo percorso di adattamento progressivo delle due dimensioni dev'essere veloce quanto l'innovazione tecnologica».

La dimensione della rete è globale, quella giudiziaria e di protezione della privacy è nazionale. Si possono perseguire soggetti formalmente stranieri come facebook?

«Con sentenze fondamentali e con il nuovo regolamento UE di protezione dei dati, la giurisprudenza europea assoggetta le società extra-europee al nostro ordinamento quando trattino dati di cittadini europei. Ma gli stessi gestori dei social network hanno interesse a presentarsi agli occhi degli utenti non come nemici. C'è un fiorire di disponibilità che vedremo quanto concrete».

Niente controllo preventivo sui contenuti?

«Sarebbe terribile delegare la censura a queste organizzazioni gigantesche largamente governate da algoritmi. Il tema della libertà di opinione mai come in questo caso verrebbe a scontrarsi con una necessità di tutela dei diritti. Nessun ruolo di filtro preventivo generico possiamo attribuire ai motori di ricerca se non forse, tramite selettori, in casi molto mirati e specifici di istigazione all'odio».

Il problema di Tiziana nasce con l'innesco della diffusione virale...

«Diffondere in rete un dato ricevuto nel nostro smartphone senza il consenso di chi ce lo ha trasmesso è un illecito sanzionato dal codice in materia di privacy, e se contiene profili di diffamazione è anche un reato penale. Non sono in grado di valutare quanto nella vicenda tristissima di Tiziana ci fosse nella diffusione dei video un intento tale da configurare il reato penale, ma l'illecito c'era. E spero che si possa aprire una finestra sul rischio corso da chi ingenuamente o no consegna alla rete i propri dati, ma anche da chi li diffonde».

I provider devono essere comunque più solleciti nella rimozione?

«Noi come Autorità siamo molto determinati a far valere concretamente il nostro ordinamento verso tutti gli internet provider, e abbiamo dalla nostra molte sentenze della Corte di giustizia europea che ci incoraggiano».

E se l'FBI o la magistratura chiedono a un'azienda come Apple di "aprire" gli smartphone di terroristi o criminali?

«Apple con l'FBI ha forzato il buonsenso: si chiedeva a chi detiene il codice sorgente di aprire non tutte ma alcune 'casseforti', in nome della collaborazione contro crimine e terrorismo. È successo anche a Milano. Atteggiamenti di resistenza a un percorso di legalità che invece conviene a tutti. In questi casi, mi auguro in futuro una collaborazione intelligente dei provider».

Marco Ventura

«A NAPOLI E MONACO SI IMPUTA A FACEBOOK L'OMESSA RIMOZIONE L'OSCURAMENTO NON PUÒ SEGUIRE PROCEDURE LUNGHE»

«VITA FISICA E DIGITALE VANNO TRATTATE SULLA BASE DEGLI STESSI OBBLIGHI E DEGLI STESSI DIRITTI»

IL MATTINO

Data 07-11-2016
Pagina 11
Foglio 1

«Google elimina i contenuti nocivi ma ognuno protegga il suo account»

Intervista

Stazi: sicurezza e privacy si tutelano anche attraverso comportamenti responsabili

Gigi Di Fiore

Docente di diritto dell'informatica all'Università Luiss di Roma, il professore Andrea Stazi è Public policy manager di Google. È a Napoli, dove oggi pomeriggio parteciperà al convegno sulla tutela dei minori nel mondo digitale all'Università Federico secondo dove sarà anche il presidente dell'Autorità per la tutela della privacy, Antonello Soro.

Professore Stazi, come nasce il confronto tra esperti in programma oggi all'Università di Napoli?

«È un'altra tappa di una campagna di sensibilizzazione all'uso responsabile della Rete, rivolta soprattutto ai giovani, con particolare attenzione alla tutela della privacy. Ne è promotore Google, con Altro consumo, la Polizia postale e l'Accademia italiana del codice di Internet».

Una campagna che prevede solo confronti pubblici tra docenti ed esperti?

«Non solo. Certo, a Napoli e poi il giorno successivo a Salerno, parleranno una serie di docenti e studiosi dei problemi legati all'utilizzo di Internet. Poi, come nell'ultimo fine settimana, siamo presenti in una grossa piazza con un camion di Google, invitando la gente a controllare la sicurezza del proprio account. A Napoli, siamo stati in piazza Dante. La verifica dell'account Google dei passanti interessati prevedeva eventuali suggerimenti e correttivi, a tutela della privacy del singolo utente».

È vero che l'espansione della Rete ha reso ormai non più rinviabile una rigorosa educazione, partendo da un'età molto giovane?

«Ne siamo fermamente convinti. La sicurezza e il rispetto della privacy sono i due temi caldi nell'uso della Rete. Sono temi che a noi particolarmente cari».

Qual è la posizione di Google rispetto a contenuti pubblicati in Rete, che risultano nocivi ad un utente?

«Rispettiamo le imposizioni di provvedimenti giudiziari e del garante della privacy. Gli utenti possono segnalare contenuti attraverso gli appositi strumenti che Google mette a disposizione e verranno rimossi se sono in violazione delle politiche (policy) di YouTube».

L'utente può quindi ormai chiedere con successo la rimozione di notizie, video e foto che considera per lui dannosi e illeciti?

«Le richieste di rimozione vengono vagliate con attenzione e rimosse qualora rispecchino i criteri definiti dalla Corte di Giustizia Europea per il cosiddetto 'diritto all'oblio'. Ma c'è da tener presente che un altro aspetto, da noi ritenuto fondamentale, è la gestione del proprio account in maniera responsabile e sicura. Ognuno può ed è importante che sia in grado di gestire i propri dati personali attraverso lo strumento Account Personale, da noi messo a disposizione».

Non molto tempo fa, proprio Google fu destinataria di una sentenza innovativa, sul diritto all'oblio. Che ne pensa?

«Non commento sentenze, ma ormai il meccanismo del riconoscimento del diritto all'oblio in particolari condizioni è entrato nella gestione di Google. Sin dal 2011 abbiamo poi ammesso la portabilità dei dati, oggi prevista anche dal regolamento dell'Unione europea in materia di privacy».

Pensa che i provider, che offrono delle loro piattaforme agli utenti per la pubblicazione di dati sensibili, debbano verificare in anticipo cosa viene diffuso, proprio come sono obbligati a fare i direttori di testate giornalistiche?

«Il controllo preventivo dei contenuti sulle piattaforme dei social, paragonabile ad una censura, viene escluso da tempo dalle discipline europee in materia».

È vero, come sostengono alcuni esperti di informatica e tecnici dell'uso della Rete, che anche eliminato da un sito originario un post non verrà mai del tutto cancellato da Internet?

«È un aspetto molto dibattuto dai tecnici informatici, con pareri assai discordi. È comunque possibile chiedere la rimozione anche dal sito originario».

Si è radicato un utilizzo selvaggio della Rete, che sembra quasi sfuggire a qualsiasi regola?

«Internet è uno strumento che offre grandi opportunità. Gli utenti hanno talora un atteggiamento leggero verso la Rete. L'obiettivo di questa nostra campagna in giro per l'Italia è proprio quello di un'educazione diffusa dei cittadini e dei più giovani a come comportarsi e cautelarsi nell'accesso a Internet».

La maggior parte degli utenti crede che il mondo virtuale sia del tutto scollegata dalla realtà e quindi che in Rete tutto sia permesso?

«Non è così, anche su Internet vigono delle regole e l'educazione al loro rispetto è fondamentale».

L'oblio
Riconosciuto come diritto dal motore di ricerca e sin dal 2011 i dati posso essere trasferiti

La campagna
A Napoli siamo stati in piazza Dante e saremo a Salerno per parlare con i docenti

la Repubblica

Data 08-11-2016
Pagina 1
Foglio 1 / 2

Il vademecum del Garante sull'utilizzo dei dati personali, soprattutto quando si usa la tecnologia
Ecco le indicazioni più preziose per far valere i propri diritti e rispettare quelli altrui

La privacy in classe

Dai video della gita alle pagelle come difendere la riservatezza

CRISTINA NADOTTI

ROMA. La foto della gita scolastica postata su Facebook, la chat con le mamme per informarsi sulla recita all'asilo, il menu della mensa con la pietanza esotica su Instagram. Un click e tutto finisce in rete, senza pensare se sia lecito o meno. Ora il Garante per la privacy dà una lezione a scuole, famiglie e alunni, per richiamare tutti a una maggiore consapevolezza nel trattamento dei dati personali, soprattutto quando si usa la tecnologia. È nato per questo *A scuola di privacy*, il vademecum elaborato dall'Autorità che sarà inviato a tutti gli istituti pubblici e privati in formato digitale e che può essere richiesto da chiunque anche in forma cartacea.

«Le scuole sono chiamate ogni giorno ad affrontare la sfida più difficile, quella di educare le nuove generazioni non solo alla conoscenza di nozioni basilari e alla trasmissione del sapere, ma soprattutto al rispetto dei valori fondanti di una società — ha sottolineato il presidente Soro nel presentare il vademecum — È importante riaffermare quotidianamente, anche in ambito scolastico, quei principi di civiltà, come la riservatezza e la dignità della persona, che devono sempre essere al centro della formazione di ogni cittadino».

In 40 pagine, il Garante ribadisce il ruolo della scuola nell'educazione alla difesa della privacy e individua proprio nei giovani «che rappresentano spesso l'avanguardia tecnologica» anche i soggetti più esposti ad abusi, al cyberbullismo, alle discriminazioni. Soprattutto a loro, ma non solo, si rivolge il decalogo per renderli consapevoli che «le proprie azioni in rete possono produrre effetti negativi anche nella vita reale e per un tempo indefinito». Perché per un click basta un secondo, ma per cancellarne gli effetti a volte non è sufficiente una vita. Ecco alcune delle indicazioni più preziose contenute nel vademecum, utili per far valere i propri diritti e rispettare quelli altrui a scuola.

LE REGISTRAZIONI

Si possono registrare video e audio a scuola?

Sì, nel rispetto delle libertà individuali e rispettando eventuali altre indicazioni della scuola. Il Garante sottolinea che «l'utilizzo di telefoni cellulari, di apparecchi per la registrazione di suoni e immagini è in genere consentito, ma esclusivamente per fini personali, e sempre nel rispetto dei diritti e delle libertà fondamentali delle persone coinvolte (siano essi studenti o professori) in particolare della loro immagine e dignità». È uno dei punti chiave del vademecum, che ha tra gli obiettivi principali (c'è un paragrafo intitolato proprio "Cyberbullismo e altri fenomeni di rischio") di porre un argine alla diffusione di immagini lesive della dignità dei ragazzi più deboli. L'opuscolo ricorda però che l'ultima parola spetta alla scuola che può «regolare o inibire l'utilizzo di registratori, smartphone, tablet e altri dispositivi elettronici all'interno delle aule o nelle scuole stesse».

LE RECITE E LE GITE

Si possono registrare e diffondere video e immagini di recite e gite scolastiche?

Sì, ma a patto che le si veda soltanto in ambito familiare e che si faccia attenzione alla loro diffusione su Internet e sui social. Vale in genere la regola aurea del chiedere il consenso alle persone che vi appaiono. «Non violano la privacy le riprese video e le fotografie raccolte dai genitori durante le recite, le gite e i saggi scolastici — è l'indicazione data dal Garante — Le immagini, in questi casi, sono raccolte per fini personali e destinate a un ambito familiare o amicale e non alla diffusione. Va però prestata particolare attenzione alla eventuale pubblicazione delle medesime immagini su Internet, e sui social network in particolare. In caso di comunicazione sistematica o diffusione diventa infatti necessario, di regola, ottenere il consenso informato delle persone presenti nelle fotografie e nei video».

I TEMI

Se l'insegnante legge in classe un tema sulla famiglia dello studente, viola la sua privacy?

È capitato a tutti di veder spiattellare nel tema "Parlo della mia famiglia", assegnato dalla maestra, questioni più o meno private o che comunque si sarebbero volentieri tenute tra le mura domestiche. «Non lede la privacy l'insegnante che assegna ai propri alunni lo svolgimento di temi in classe riguardanti il loro mondo personale o familiare — specifica il vademecum — Nel momento in cui gli elaborati vengono letti in classe — specialmente se riguardano argomenti delicati — è affidata alla sensibilità di ciascun insegnante la capacità di trovare il giusto equilibrio tra le esigenze didattiche e la tutela dei dati personali. Restano comunque validi gli obblighi di riservatezza già previsti per il corpo docente riguardo al segreto d'ufficio e professionale, nonché quelli relativi alla conservazione dei dati personali eventualmente contenuti nei temi degli alunni».

GLI ESAMI

I voti e i risultati degli esami sono pubblici?

Su questo punto il Garante torna dopo un lungo dibattito che aveva infiammato gli ambienti scolastici soprattutto a proposito dell'affissione dei risultati nelle bacheche degli istituti. «Gli esiti degli scrutini o degli esami di Stato sono pubblici — ribadisce l'opuscolo — Le informazioni sul rendimento scolastico sono soggette a un regime di conoscibilità stabilito dal ministero dell'Istruzione dell'Università e della Ricerca. È necessario però che, nel pubblicare i voti degli scrutini e degli esami nei tabelloni, l'istituto scolastico eviti di fornire, anche indirettamente, informazioni sulle condizioni di salute degli studenti, o altri dati personali». Non devono mai essere pubblici gli esiti di prove differenziate sostenute da studenti portatori di handicap o con disturbi specifici di apprendimento. Questo tipo di voti sono indicati soltanto nell'attestazione da rilasciare allo studente.

la Repubblica

Data 08-11-2016
Pagina 1
Foglio 2 / 2

LE CHAT TRA GENITORI

Le comunicazioni scolastiche possono ledere la riservatezza?

Sì, se segnalano l'identità di alunni coinvolti in casi di bullismo o vicende delicate. Nel vademecum elaborato dall'Autorità non c'è un capitoletto specifico per le chat tra genitori, di recente diventate argomento per fatti di cronaca, ma l'intento di sensibilizzare a un uso consapevole di questi strumenti è chiaro. Si dice che si deve prestare attenzione «a comportamenti anomali e fastidiosi su un social network, su sistemi di messaggistica istantanea (come Whatsapp, Snapchat, Skype, Messenger, etc.)». E soprattutto si ammonisce che «il diritto-dovere di informare le famiglie sull'attività e sugli avvenimenti della vita scolastica deve essere sempre bilanciato con l'esigenza di tutelare la personalità dei minori». Perciò non vanno mai inseriti dati personali che rendano identificabili, ad esempio, gli alunni coinvolti in casi di bullismo o in altre vicende particolarmente delicate.

I SOCIAL

Si possono pubblicare sui social video e foto fatti in aula?

No, a meno che non si sia chiesta l'autorizzazione alle persone che vi appaiono. L'intento è chiaro: ognuno è padrone della propria immagine e anche quando si postano sui social foto che riprendono situazioni positive bisognerebbe chiedere l'autorizzazione. «Si deve prestare particolare attenzione prima di caricare immagini e video su blog o social network — ammonisce l'opuscolo — oppure di diffonderle attraverso mms o sistemi di messaggistica istantanea. Succede spesso, tra l'altro, che una fotografia inviata a un amico o a un familiare venga poi inoltrata ad altri destinatari, generando una comunicazione a catena dei dati personali raccolti. Tale pratica può dar luogo a gravi violazioni del diritto alla riservatezza delle persone riprese, e fare incorrere in sanzioni disciplinari, pecuniarie e in eventuali reati».

LE LEZIONI

Si può registrare o riprendere un professore mentre fa lezione?

Sì, ma video e audio non possono essere diffusi su Internet e i contenuti devono essere usati solo per motivi di studio personali. In ogni caso la scuola, e in particolare l'insegnante che viene ripreso nel video, devono essere informati. Al Garante non sfugge però il possibile valore didattico di questi strumenti e ne specifica meglio l'uso in alcune situazioni: «Nell'ambito dell'autonomia scolastica, gli istituti possono decidere di regolamentare diversamente o anche di inibire l'utilizzo di apparecchi in grado di registrare. In ogni caso deve essere sempre garantito il diritto degli studenti con diagnosi Dsa (disturbi specifici dell'apprendimento) o altre specifiche patologie di utilizzare tutti gli strumenti compensativi (come il registratore) di volta in volta previsti nei piani didattici personalizzati che li riguardano».

LE MENSE

Si possono rendere pubblici particolari sul servizio mensa?

Spesso non ci si pensa, ma anche il menu della mensa può rivelare dati personali. «Alcune particolari scelte, infatti (pasti vegetariani o rispondenti a determinati dettami religiosi) possono essere idonee a rivelare le convinzioni (religiose, filosofiche o di altro genere) dei genitori e degli alunni» osserva il Garante, che sottolinea in modo particolare che non si possono affiggere sulla bacheca della scuola i nomi degli alunni genitori dei quali non hanno provveduto al pagamento della retta per il servizio o che hanno esenzioni per reddito. «Eventuali buoni pasto, tra l'altro, non possono avere colori differenziati in relazione alla fascia di reddito di appartenenza delle famiglie». Attenzione anche al servizio di scuolabus: mai pubblicare online o in bacheca gli elenchi di chi lo usa o delle fermate di salita e discesa per non esporre sia le famiglie, sia i piccoli a rischio malintenzionati.

Il Sole 24 ORE

Data 14-11-2016
Pagina 21
Foglio 1

INNOVAZIONE & TUTELA DEI DATI PERSONALI

La sfida della sicurezza «social»

Lotta al crimine online e privacy in cerca di un difficile equilibrio

di **Susanna Sandulli**

Una delle tematiche più ricorrenti degli ultimi anni riguarda la tutela della sicurezza nello svolgimento delle attività online; se tale questione, da una parte, concerne indubbiamente la lotta al terrorismo internazionale e la repressione di altri reati come la pedopornografia, notevoli problemi si pongono a causa dello sviluppo dei social networks, in quanto la sicurezza pubblica può essere minacciata da diverse forme di cybercrime.

Il fulcro della questione è ravvisabile nelle ripercussioni economiche che tali fattispecie di reato possono produrre, poiché nella Rete sono presenti molti dati riguardanti imprese o patrimoni individuali e, pertanto, la cosiddetta business continuity è sottoposta a un forte rischio.

La necessità di una maggior implementazione dei sistemi di sicurezza è stata sottolineata anche dall'Ocse (Organizzazione per la cooperazione e lo sviluppo economico), la quale, tramite la raccomandazione sulla sicurezza digitale e la gestione del rischio del 1° ottobre 2015, ha evidenziato che essa si pone come un problema non solamente di ordine tecnologico, ma anche economico.

Come rimarcato dal presidente del Garante per la tutela dei dati personali, Antonello Soro, non è pensabile eliminare del tutto i rischi derivanti dal digitale e, in un certo senso, questi devono essere accettati in ragione dei plurimi obiettivi che l'Italia e l'Unione europea si sono poste; tuttavia, ciò non può esonerare i governi dei singoli Stati dall'adottare una serie di strategie che assicurino la tutela della privacy dei cittadini, conferendo a quest'ultima il ruolo di obiettivo primario dei piani di sviluppo.

L'innovazione, infatti, a parere dell'Ocse, deve essere considerata un aspetto fondamentale nell'attività di gestione della sicurezza digitale, la quale, per essere efficiente, deve garantire una piena collaborazione non solo tra soggetti pubblici e privati, ma anche fra i diversi Stati, dando vita a una compenetrazione fra diritto nazionale e sovranazionale.

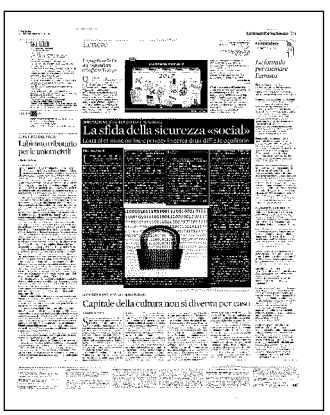
Infine, sebbene la digital security influenzi profondamente il raggiungimento dei diversi obiettivi economici e sociali, essa deve andare sempre di pari passo con la salvaguardia dei diritti fondamentali, affinché la tutela di questi non risulti, in alcun modo, diminuita.

A partire dagli eventi dell'11 settembre 2001 e a seguito dei, purtroppo, numerosi attentati terroristici che sono stati realizzati in Europa negli ultimi anni, la necessità di una maggior sicurezza ha comportato un'ingerenza notevole di dati personali che potrebbe ledere quel sistema di protezione così difficilmente realizzato; pertanto, la Corte di giustizia ha sottolineato la necessità che il controllo sui dati personali degli utenti per ragioni di sicurezza incontri limiti ben precisi.

Proprio per questo, il 6 luglio 2016 sono state approvate dal Parlamento europeo le norme relative alla strategia sulla sicurezza informatica («Cyber security») e fra queste anche la direttiva Nis (Network and Information Security), applicabile a tutti i soggetti che svolgono attività ascrivibili ai cosiddetti servizi essenziali; essa nasce dalla consapevolezza che il sistema moderno si caratterizza per una logica di interoperabilità dei servizi, la quale aumenta in maniera esponenziale i rischi e, infatti, la direttiva, oltre a imporre agli Stati membri di riferire a un'apposita Autorità nazionale i vari incidenti che si verificano, obbliga questi ultimi a istituire il Cert (Computer emergency response team), ossia un network che si occupi delle reti più critiche, monitorando gli eventuali incidenti verificatisi a livello nazionale.

Sebbene, dunque, la sicurezza e la privacy degli internauti costituiscano uno dei più importanti obiettivi che l'Ocse si è prefissata di raggiungere mediante l'instaurazione di un clima di maggior fiducia, è innegabile che, in realtà, giungere alla creazione di un diverso e migliore mosaico giuridico, comunitario e internazionale, sia un risultato estremamente ambizioso; infatti, oltre che delle indubbie difficoltà applicative, è necessario tener conto anche dei diversi valori che caratterizzano gli Stati, europei e non.

L'articolo è un estratto dal capitolo «Privacy e sistema social» contenuto nel rapporto «Consumerism 2016» (giunto alla nona edizione) realizzato da Consumers' Forum, in collaborazione con l'Università degli studi di Roma Tre e coordinato da Liliana Rossi Carleo e Fabio Bassan, rispettivamente professore emerito di Diritto privato e professore ordinario di Diritto internazionale presso lo stesso ateneo


La sfida della sicurezza «social»

Il Sole 24 ORE

Data 22-11-2016
Pagina 10
Foglio 1

FOCUS. I RISCHI NELLA PA

La cybersecurity sconta il deficit di prevenzione

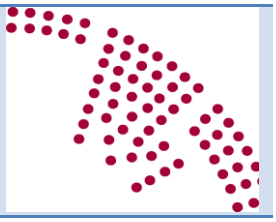
Biagio Simonetta

Prima un sito del dipartimento di Funzione pubblica hackerato da un 17enne, poi il portale di Equitalia che rimane inaccessibile per ore a causa di un cyber-attacco. Sono stati giorni turbolenti, gli ultimi, per la sicurezza informatica italiana. Due episodi, che però ripropongono un discorso quanto mai aperto: le vulnerabilità dell'Italia digitale. Se da un lato, infatti, la digitalizzazione del Paese sembra un obiettivo in ritardo ma concreto, dall'altro aleggiano interrogativi pesanti. Siamo veramente pronti a un'Italia digitale? O rischiamo di scoprire il fianco ai cybercriminali di mezzo mondo, sempre più affamati di dati? Lo abbiamo chiesto ad Andrea Rigoni, partner di Deloitte e membro dell'unità di missione per l'attuazione dell'Agenda digitale durante il governo Letta.

«Questi due attacchi – racconta Rigoni al Sole 24 Ore – sono due cartine di tornasole. Chiariamolo subito: di per sé non siamo davanti a due incidenti gravi, perché chi conosce l'ambito cyber sa che può succedere decisamente di peggio. Tuttavia sono due indicazioni preoccupanti. Due episodi che ci dicono alcune cose. Ci dicono innanzitutto che manca un processo di base in grado di garantire la sicurezza. Le lacune sono evidenti, e indicano una carenza sistemica grave che - in virtù di quello che è successo - ci porta a pensare che la situazione sia analoga un po' per tutti i siti/servizi della Pa. Il quadro diventa ancora più allarmante se si considera, poi, che la pubblica amministrazione è uno dei target più appetibili (insieme a quello militare, finanziario ed energetico) per i cyber criminali».

Preoccuparsi, insomma, è il minimo. E nell'immediato il cielo non sembra schiarirsi: «Metterci al riparo dall'oggi al domani non è un processo semplice» aggiunge Rigoni, secondo quale «manca una politica di prevenzione e preparazione (la cosiddetta "readiness")». E del resto, «basta guardare i fondi pubblici stanziati per la sicurezza informatica per capire cosa sto dicendo: a fronte di una digitalizzazione dilagante, di processi di Industry 4.0 che diventano sempre più concreti, si investe pochissimo in sicurezza». Quello che manca, dunque, «è il concetto di prevenzione e la capacità di avere un'analisi che ci avvisi di ciò che sta succedendo quando siamo ancora in tempo. Ad oggi non siamo in grado di stabilire quanti attacchi silenti siano in atto sui portali della Pa». Già, proprio così: silenti. Essere sotto attacco e non accorgersene è qualcosa che accade di frequente.

Elenco delle ultime rassegne tematiche
Pubblicate e disponibili presso l'archivio



2016

35	10/11/2016	16/11/2016	ELEZIONI USA: L'EUROPA DOPO TRUMP
34	4/10/2016	17/11/2016	ELEZIONI USA E CYBERPROPAGANDA
33	7/8/2016	14/11/2016	LA SITUAZIONE IN TURCHIA
32	9/11/2016	14/11/2016	UMBERTO VERONESI
31	18/10/2016	9/11/2016	IL REFERENDUM COSTITUZIONALE (II)
30	16/09/2016	9/11/2016	LA BATTAGLIA DI MOSUL
29	31/10/2016	7/11/2016	IL TERREMOTO IN CENTRO ITALIA
28	06/09/2016	24/10/2016	IL CONFLITTO SIRIANO
27	15/10/2016	22/10/2016	LA RISOLUZIONE UNESCO SU GERUSALEMME
26	13/09/2016	21/09/2016	I CONFRONTI TRA I CANDIDATI ALLA PRESIDENZA USA
25	28/09/2016	21/10/2016	LA MANOVRA ECONOMICA 2017
24	27/09/2016	17/10/2016	IL REFERENDUM COSTITUZIONALE
23	01/08/2016	25/09/2016	LA RIFORMA DEL SENATO (XV)
22	29/09/2016	03/10/2016	LA MORTE DI SHIMON PEREZ
21	17/09/2016	19/09/2016	CARLO AZEGLIO CIAMPI
20	16/07/2016	05/08/2016	LA CRISI TURCA
19	23/03/2016	02/0872016	LA LOTTA AL TERRORISMO
18	11/03/2016	02/08/2016	LA POLITICA EUROPEA DELL'IMMIGRAZIONE (III)
17	23/06/2016	28/07/2016	LA RIFORMA DEL SENATO (XIV)
16	10/04/2016	28/06/2016	RIFORMA DELLE PENSIONI
15	31/05/2016	27/06/2016	BREXIT (II)
14	14/04/2016	22/06/2016	LA RIFORMA DEL SENATO (XIII) (vol. 1 e vol. 2)
13	31/12/2015	31/05/2016	MAGISTRATURA E POLITICA
12	01/01/2016	30/05/2016	BREXIT
11	20/05/2016	24/05/2016	LA MORTE DI MARCO PANNELLA
10	01/03/2016	23/05/2019	IL DIBATTITO SULLE ADOZIONI
09	02/01/2016	17/05/2019	LA RIFORMA DEL PROCESSO PENALE
08	01/03/2016	16/05/2016	IL DDL SULLE UNIONI CIVILI (V)
07	09/03/2016	03/05/2016	LA CRISI IN LIBIA (II)
06	20/10/2015	15/04/2016	LA RIFORMA DEL SENATO (XII)
05	11/12/2015	10/03/2016	LA POLITICA EUROPEA DELL'IMMIGRAZIONE (vol. 2)
05	14/06/2015	10/12/2015	LA POLITICA EUROPEA DELL'IMMIGRAZIONE (vol. 1)
04	01/01/2016	08/03/2016	LA CRISI IN LIBIA
03	10/02/2016	01/03/2016	IL DDL SULLE UNIONI CIVILI (IV)
02	15/10/2015	09/02/2016	IL DDL SULLE UNIONI CIVILI (III)
01	01/12/2015	31/12/2015	IL CONFLITTO SIRIANO (II)

2015

44	20/11/2015	30/11/2015	IL CONFLITTO SIRIANO (vol. 2)
44	01/11/2015	19/11/2015	IL CONFLITTO SIRIANO (vol. 1)
43	21/10/2015	19/11/2015	LA LEGGE DI STABILITA' 2016
42	31/07/2015	18/11/2015	IL PIANO PER IL SUD
41	01/07/2015	06/11/2015	RAPPRESENTANZA SINDACALE E RIFORMA DEI CONTRATTI
40	25/07/2015	27/10/2015	LA REGOLAMENTAZIONE DEL DIRITTO DI SCIOPERO
39	01/10/2015	20/10/2015	VERSO LA LEGGE DI STABILITA' (vol.2)
39	19/07/2015	30/09/2015	VERSO LA LEGGE DI STABILITA' (vol.1)
38	09/10/2015	19/10/2015	LA RIFORMA DEL SENATO (XI)
37	03/07/2015	14/10/2015	IL DDL SULLE UNIONI CIVILI (II)
36	26/09/2015	08/10/2015	LA RIFORMA DEL SENATO (X)
35	16/09/2015	25/09/2015	LA RIFORMA DEL SENATO (IX)
34	25/08/2015	15/09/2015	LA RIFORMA DEL SENATO (VIII vol. 2)