PRIVACY

Tecnologie del controllo e privacy: evoluzione o rivoluzione?

LINUX DAY
TORINO
28.10.2017
linuxdaytorino.org

Prof. Avv. Camillo Sacchetto

2005

2013
NBC NEWS

2015: sorpasso…

nel 2010 è stata creata una quantità di dati superiore a quella prodotta complessivamente dall'uomo negli ultimi 30.000 anni di storia.
(Eric Schmidt)

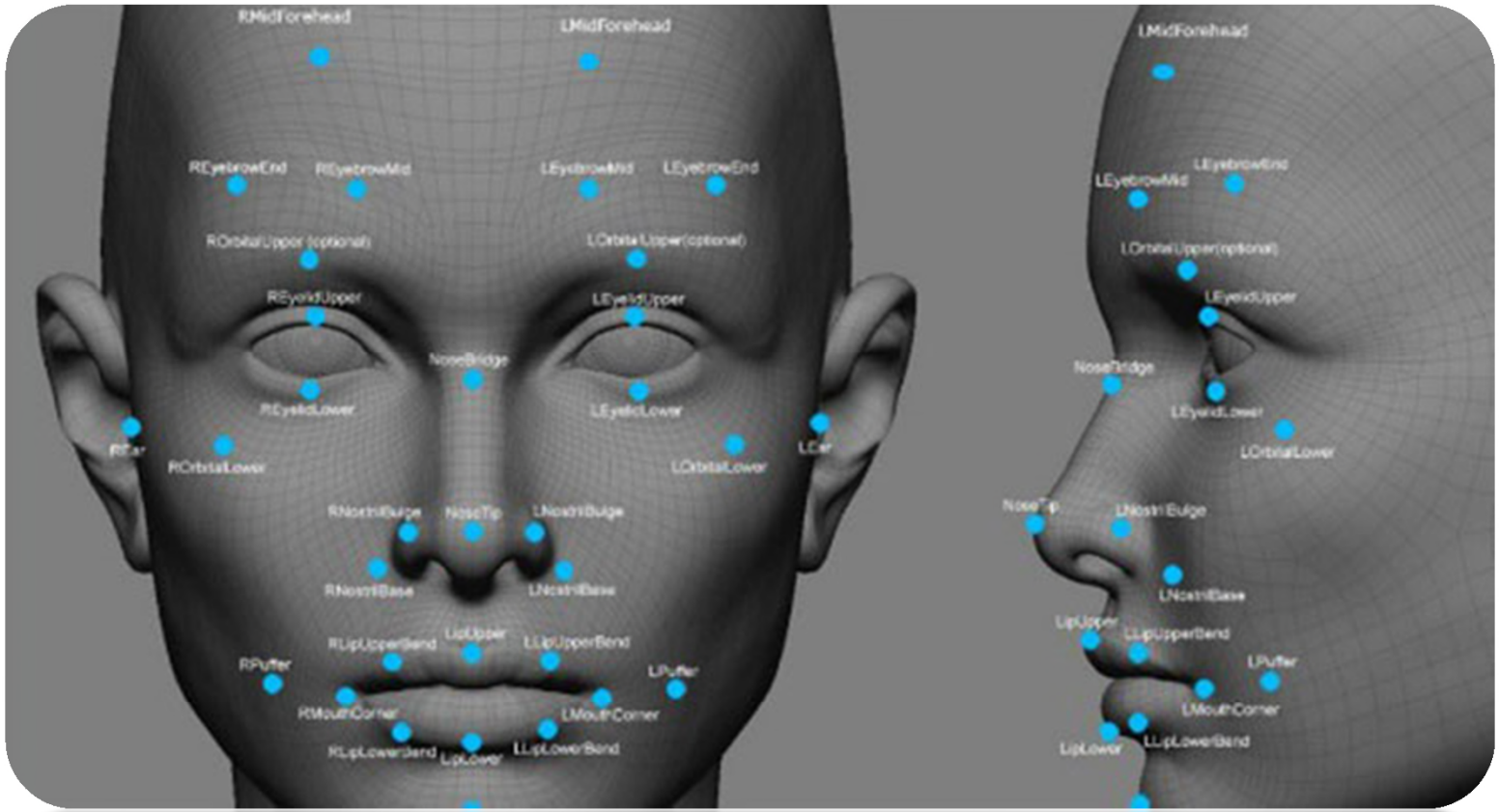
Commissione Europea, *Verso una florida economia basata sui dati*, COM(2014) 442, 2014/07/02.

Do You Know Where Your Data Is?

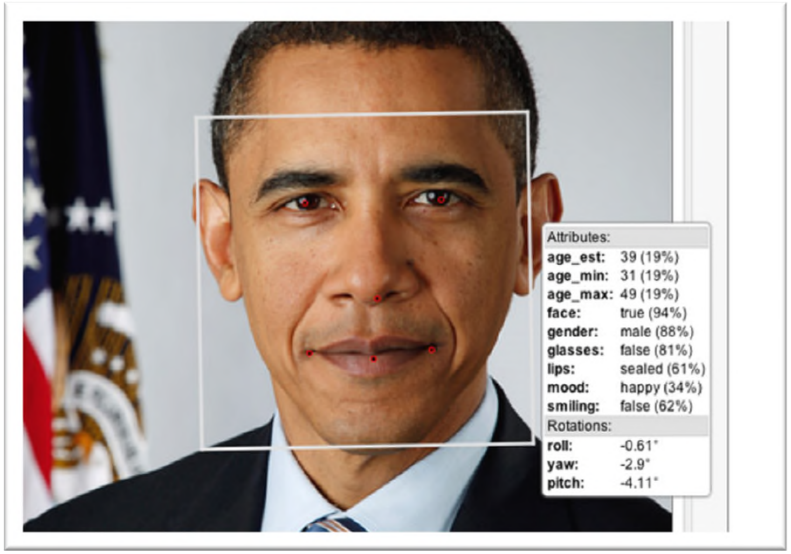
ROSITA, QUALE COOKIE
È TECNICO E QUALE DI
PROFILAZIONE?

Privacy e... controllo biometrico

Privacy e…riconoscimento facciale



Face.com & Facebook



Testo associato:	la tua immagine del profilo, L'immagine può contenere: 1 persona, in piedi, barba e spazio al chiuso

Facedeals

facedeals
Face detected
Face saved /tmp/face-yNbFE.png
Initializing OpenCV with Facedeals user templates
Template matching /tmp/face-yNbFE.png...
Facebook user 560585484 matched with 98.072% confidence
Checking in https://graph.facebook.com/560585484/checkins...
Getting likes https://graph.facebook.com/560585484/likes...
Getting current deals for place 57889082694
Optimizing deal for user 560585484...
Dispatching mobile notification...

Profilazione Marketing

SHORE

Sophisticated High-speed Object Recognition Engine

Questo accadeva nel 1893…

Scheda manicomiale di "*pederasta*" (Almè Ettore), datata 17/171893, dal "Museo Lombroso" di Torino (http://www.giovannidallorto.com/saggistoria/nonno/nonno.html)

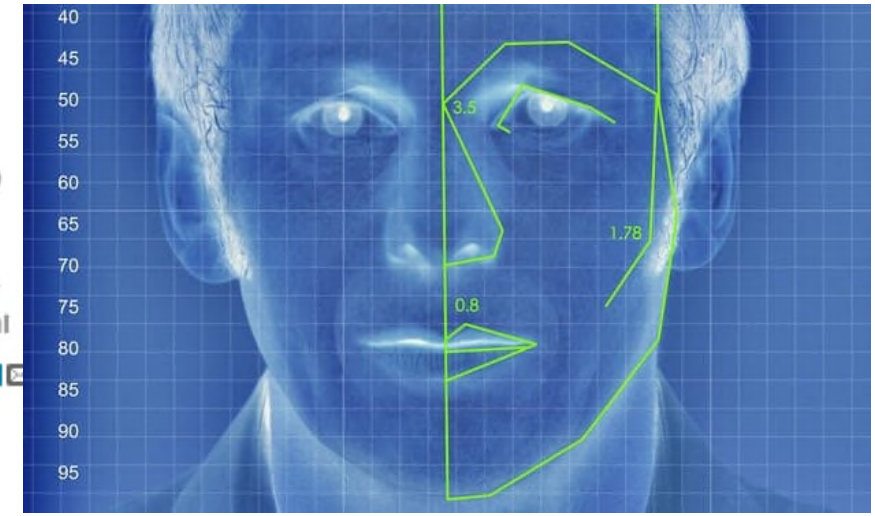
E questo nel 2017…

Scienza e tecnologia

Sarà possibile capire se una persona è gay solo dal suo viso

Una controversa ricerca dell'Università di Stanford ha analizzato 35mila immagini facciali riprese da un sito di incontri rivelando che le persone omosessuali hanno una serie di caratteristiche fisiche comuni

08 Set. 2017



https://www.tpi.it/2017/09/08/gay-etero-algoritmo/#r

Privacy e...controllo dei lavoratori

Art. 4 – S.L. (testo originario)

Impianti audiovisivi.

1) È vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori.

Art. 4 – S.L. (testo originario)

2. Gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna.

In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti.

Ratio della normativa

- Vieta i controlli "occulti" (subdoli) sull'attività lavorativa da parte di persone non conosciute come "controllori" dal lavoratore.

- Tutela della dignità e libertà del lavoratore.

Contenuto del divieto

- È sufficiente che le apparecchiature siano state **solo installate** anche se non ancora funzionanti (Cass. 9211/97);

- concetto di **attività lavorativa**: qualsiasi attività svolta sul luogo di lavoro, anche durante le pause;

Modalità di controllo «occulte» legittime

1) nei limiti del controllo delle condotte illecite del lavoratore estranee all'attività lavorativa
(cd. "controlli difensivi" - Cass. n. 26991/09)

*2) su addetti alle casse **da parte di investigatori** che, operando come clienti si limitano a presentare alle casse la merce acquistata e a pagare il relativo prezzo verificando la mancata registrazione della vendita e l'appropriazione della somma incassata da parte del lavoratore (Cass. 20613/2012)*

Rilevanza del consenso dei lavoratori

Irrilevante l'eventuale consenso dei singoli lavoratori ovvero la conoscenza del controllo

(Cass. 9211/97)

Controlli ammessi dalla giurisprudenza

Controlli cd. "difensivi" al fine di dimostrare l'illecito posto in essere da propri dipendenti, utilizzando le risultanze di **registrazioni video operate fuori dall'azienda** **da un soggetto terzo** o **i tabulati telefonici acquisiti da un soggetto terzo**, del tutto estraneo all'impresa e ai lavoratori dipendenti della stessa, con la conseguenza che tali risultanze sono legittimamente utilizzabili nel processo dal datore di lavoro.

(Cass. 5371/2012; Cass. 2117/2011)

Segue...

- È legittimo il licenziamento dell'addetto di sorveglianza che durante il turno usa il telefono per ore (Cass. n. 5371/2012)

- È legittimo il controllo *ex post* su messaggi di posta elettronica in presenza di sospetti su illeciti (Cass. 2722/2012)

Provvedimento Garante Privacy (2007):
principi generali su accesso a internet e utilizzo delle e-mail nei luoghi di lavoro

- La proprietà del mezzo di lavoro (computer aziendale) nonché della dorsale informatica e dell'accesso ad internet rimane in capo al datore di lavoro;

- il lavoratore non è titolare di alcun diritto di accesso ad internet né di utilizzo della posta elettronica;

- il datore dunque può regolamentare l'accesso ad internet, e persino vietarlo (mediante un chiaro protocollo aziendale sulle regole di accesso ad internet), ma un divieto assoluto non è razionalmente concepibile;

Segue...

- In luogo di un divieto assoluto, si propone un divieto selettivo, che riguardi: siti non pertinenti all'attività lavorativa; siti a pagamento; siti l'accesso ai quali è disdicevole (siti porno, che inneggiano a discriminazioni ecc.); il download di programmi o file non autorizzati, al di fuori della rete aziendale Intranet o dei siti Internet certificati;

- è possibile ricorrere a misure preventive (filtri) che consentano l'accesso solo a certi siti e/ o solo in certe fasce orarie (ad es. nelle pause dei lavoro);

- il datore può vietare l'uso della posta per fini personali, o limitarlo (come è più ragionevole ipotizzare).

La prova nel processo penale.

Cass. Pen. Sez. 2 n. 2890/2015

Sono utilizzabili nel processo penale, ancorché imputato sia il lavoratore subordinato, i risultati delle videoriprese effettuate con telecamere installate all'interno dei luoghi di lavoro ad opera del datore di lavoro per esercitare ***un controllo a beneficio dei patrimonio aziendale messo a rischio da possibili comportamenti infedeli dei lavoratori****, perché le norme dello Statuto dei lavoratori poste a presidio della loro riservatezza non fanno divieto dei cosiddetti controlli difensivi del patrimonio aziendale e non giustificano pertanto l'esistenza di un divieto probatorio*

Testo attuale (D.Lgs. 151/2015)

Art. 4
(Impianti audiovisivi e altri strumenti di controllo)

1. Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori **possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale** e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali.

Art 4 S.L. (testo attuale) (D.Lgs. 151/2015)

2. La disposizione di cui al comma 1 ***non si applica*** *agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.*

1. Le informazioni raccolte ai sensi dei commi 1 e 2 sono ***utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli*** *e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196.*

Testo originario Statuto dei Lavoratori

Art. 4. (Impianti audiovisivi)

i. E' vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di control o a distanza dell'attività dei lavoratori,

2. Gli impianti e le apparecchiature di controllo che siano richiesti da **esigenze organizzative e produttive ovvero dalla sicurezza del lavoro,** ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previa accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti.

1. Per gli impianti e le apparecchiature esistenti, che rispondano alle caratteristiche di cui al secondo comma del presente articolo, in mancanza di accordo con le rappresentanze sindacali aziendali o con la commissione interna, l'Ispettorato del lavoro provvede entro un anno dall'entrata in vigore della presente legge, dettando all'occorrenza le prescrizioni per l'adeguamento e le modalità di uso degli impianti suddetti.

2. Contro i provvedimenti dell'Ispettorato del lavoro, di cui ai precedenti secondo e terzo comma, il datare di lavoro, le rappresentanze sindacali aziendali o, in mancanza di queste, la commissione interna, oppure i sindacati dei lavoratori di cui al successivo art 19 possono ricorrere, entro 30 giorni dalla comunicazione del provvedimento, ai **Ministro per** il lavoro e la previdenza sociale.

Testo modificato da d.lgs. 151/2015

Art. 4 (Impianti audiovisivi e altri strumenti di controllo))

1. Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per **esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale** e possono essere installati previa accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo gli impianti e gli strumenti di **cui al** periodo precedente possono essere installati previa autorizzazione della Direzione territoriale del lavoro **o,** in alternativa, nel caso di imprese con unita' produttive dislocate negli ambiti di competenza di più Direzioni territoriali dei lavoro, del Ministero del lavoro e delle politiche sociali.

2. La disposizione di cui al comma l non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e **agli strumenti** di registrazione degli accessi e delle presenze.

3. Le informazioni raccolte ai sensi dei commi l e 2 sono **utilizzabili a tutti i** fini connessi al rapporto di lavoro a **condizione che sia** data **al lavoratore** adeguata **informazione delle** modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196,

Non fidarsi mai di una donna … inesistente

Cassazione 27 maggio 2015, n. 10955

ritenuto ammissibile il controllo “occulto” realizzato tramite la creazione di un falso profilo “*Facebook*” per acquisire la prova dell’intrattenersi del dipendente in “*chat*” con una (inesistente) signora durante l’orario di lavoro

Privacy, "spiare i social network dei candidati a un impiego è contro le regole Ue"

È quanto stabiliscono le linee guida pubblicate al "Gruppo di lavoro ex Articolo 29", organismo europeo - consultivo e indipendente - per la protezione dei dati personali

di ROSITA RIJTANO

http://www.repubblica.it/tecnologia/sicurezza/2017/07/16/news/privacy_spiare_i_social_network_dei_candidati_a_un_impiego_e_contro_le_regole_ue_-170935893/?refresh_ce

[...] Un altro, diverso, appunto riguarda i dispositivi indossabili come il Fitbit: l'azienda può fornirli ai dipendenti ma non deve collezionare i dati che ha a disposizione grazie al gadget né lavorare con terze parti che potrebbero possedere queste informazioni.

[…] Non solo, impiegati e aspiranti tali non possono essere forzati ad accettare l'amicizia social dei capi né a dare le password dei loro profili.

Si tratta di precisazioni necessarie al tempo dei social network. Quando un post su Facebook può anche costarti il licenziamento, da un lato, e precluderti opportunità lavorative, dall'altro.

Secondo un'analisi della compagnia CareerBuilder, circa il 60 percento delle imprese usa i social media per scremare i candidati.

Meeting of 10-13-16 Public Meeting on Big Data in the Workplace

Written Testimony of Ifeoma Ajunwa, J.D., Ph.D., Fellow
Berkman Klein Center at Harvard University
Assistant Professor of Law
University of the District of Columbia School of Law

Good afternoon, Chair Yang and members of the Commission. First, I would like to thank the Commission for inviting me to this meeting. My name is Ifeoma Ajunwa, I am a Fellow at the Berkman Klein Center at Harvard University and an Assistant Professor at the University of the District of Columbia School of Law. I have authored several papers regarding worker privacy, with an emphasis on health law and genetic discrimination, from which my testimony today is largely drawn.

Today, I will summarize a number of practices that employers have begun to deploy to collect information on employees, and my concerns that such information could ultimately be acquired and sold by data brokers or stored in databanks. There are few legal limitations on how this sensitive information could be used, sold, or otherwise disseminated. Absent careful safeguards, demographic information and sensitive health information and genetic information is at risk for being incorporated in the Big Data analytics technologies that employers are beginning to use -- and which challenge the spirit of antidiscrimination laws such as the Americans with Disabilities Act (the "ADA") and the Genetic Information Non-Discrimination Act ("GINA").

Use of Worker Surveillance Technologies

The technological monitoring of employees by employers is not a new phenomenon. Beginning with punch-card systems, advancing to closed-circuit video cameras, and geo-locating systems, workplace surveillance has become a fact of life for the American worker. What is novel, and of legal concern, is that with technological advancements and lowered costs, employee surveillance now occurs both inside and outside the workplace - affecting the equal access to employment for all Americans.

The potential for worker surveillance now seems limitless. For example, punch clocks have given way to thumb scans, key cards may soon give way to RFID tags, and internet browser histories are often scrutinized. Some employers log keystrokes and many are interested in capturing not only when their employees use private services like Gmail, Facebook, and Twitter, but what they publish there as well. Employer-provided cellphones, an increasingly ubiquitous piece of worker equipment, now offers employers the ability to pinpoint the worker's precise location through GPS. According to a survey from the American Management Association, at least 66 percent of U.S. companies monitor their employees' internet use, 45 percent log keystrokes, and 43 percent track employee emails. Furthermore, many workers may be unaware of the extent to which their employer is tracking them; only two states, Delaware and Connecticut, mandate that employers must inform their employees of electronic tracking.

Secondo una ricerca dell'*American Management Association*, almeno il 66% delle imprese negli USA monitorano l'uso di Internet da parte dei lavoratori, il 45% i file log elaborati dalla tastiera (i c.d. "*Keyloggers*" ricostruiscono e relazionano su tempi e quantità di battiture sulla tastiera) ed il 43% tracciano le e-mail dei lavoratori.

In questo scenario risulta che la maggior parte dei lavoratori sono ignari del monitoraggio e solamente nell'ordinamento di due Stati, il Delaware e il Connecticut, è previsto l'obbligo del datore di lavoro di informare il personale in ordine all'effettuazione del controllo.

Captatore Informatico

“captatore informatico”

Il “captatore informatico” consiste in un *software*, o, più precisamente, in un *malware* che, una volta installato (furtivamente) all’interno di un determinato sistema informatico *target*, consente ad un centro remoto di comando di prenderne il controllo, sia in termini di *download* che in termini di *upload* di dati e informazioni di natura digitale.

“captatore informatico”

- In particolare, tutte le volte in cui si parla di “captatore informatico” in ambito investigativo (c.d. *trojan* di Stato), è necessario distinguere tra *on line search* e *on line surveillance*.

- I programmi spia appartenenti alla prima categoria consentono di far copia, totale o parziale, delle unità di memoria del sistema informatico; i dati e le informazioni sono quindi trasmessi, in tempo reale o ad intervalli prestabiliti, agli organi di investigazione tramite la rete *Internet* in modalità nascosta e protetta.

“captatore informatico”

Attraverso i programmi spia che realizzano la c.d. *on line surveillance*, invece, è possibile captare il flusso informativo intercorrente tra le periferiche (video, tastiera, microfono, *webcam*, ecc.) e il microprocessore del dispositivo *target*, consentendo al centro remoto di controllo di monitorare in tempo reale tutto ciò che viene visualizzato sullo schermo (*screenshot*), digitato attraverso la tastiera (*keylogger*), detto attraverso il microfono, o visto tramite la *webcam* del sistema *target* controllato.

“captatore informatico”

I programmi spia possono essere inseriti nel sistema informatico “bersaglio” sia da remoto, attraverso l’invio di *virus trojan*, cioè programmi camuffati da innocui sms, email o applicazioni di aggiornamento che vengono scaricati e installati dall’ignaro destinatario, sia “da vicino”, intervenendo fisicamente a livello hardware sul dispositivo da controllare.

Corte Costituzionale Tedesca

Sulla questione del c.d. “captatore informatico”, si registra, il 27 febbraio 2008, la sentenza della Corte costituzionale federale tedesca, con la quale, **per la prima volta nel panorama giuridico europeo**, viene riconosciuta l’esistenza, in capo all’individuo, di **un nuovo diritto costituzionale**:

il “*diritto fondamentale alla garanzia dell’integrità e della riservatezza dei sistemi informatici*” inteso come espressione del più generale “*diritto alla dignità*” dell’individuo-utente.

Corte Costituzionale Tedesca

- Inoltre, i dati e le informazioni che gli utenti creano e conservano tramite i propri dispositivi, lungi dall'essere "neutri", hanno ad oggetto il comportamento degli utenti stessi.

- In buona sostanza, si tratta di dati da cui è possibile ricavare elementi sulla personalità dell'individuo, tracciandone un vero e proprio profilo

Corte Costituzionale Tedesca

Questo si traduce, per il legislatore, a livello di tecnica normativa, nell’obbligo del rispetto dei principi di chiarezza e sufficiente determinatezza della fattispecie, nonché nel rispetto del principio di proporzionalità.

Corte Costituzionale Tedesca

- **Chiarezza e precisione** garantiscono al cittadino la piena comprensione della legge, consentendogli di regolare la condotta in modo conforme ai precetti normativi: il legislatore deve determinare in modo chiaro e preciso i casi, le finalità ed i limiti delle eventuali restrizioni dei diritti fondamentali.

- Una tecnica legislativa basata su meri rinvii ad altre norme - al fine della individuazione dei presupposti che legittimano o meno un determinato comportamento - non rispetta il criterio di sufficiente determinatezza della fattispecie.

Corte Costituzionale Tedesca

Proporzionalità, invece, significa che una legge che preveda la compressione di diritti fondamentali deve perseguire uno scopo legittimo e ben individuato, e deve essere idonea ed opportuna quale mezzo per il raggiungimento di tale fine.

Corte Costituzionale Tedesca

«L’ incostituzionalità non riguarda, pertanto, i nuovi mezzi “di carattere tecnologico” in quanto tali ed in termini assoluti, ma (i loro modi di utilizzo) i presupposti ed i limiti, anche temporali, per la loro adozione, secondo i principi che deve seguire il legislatore nel formulare la norma, oltre che la mancata riserva, in ordine alla verifica sulla sussistenza di simili presupposti, ad un organismo indipendente e neutrale.

Cass. pen., Sezioni Unite, 28 aprile 2016 (dep. 1 luglio 2016), n. 26889

L’uso di captatori informatici nelle intercettazioni “fra presenti”

- Con questa attesa pronuncia, le Sezioni unite riconoscono la legittimità, per i delitti di criminalità organizzata, delle intercettazioni “fra presenti” anche senza la previa indicazione dei luoghi dove devono svolgersi.

- In particolare, la Cassazione ammette ufficialmente la possibilità di utilizzare a fini di surveillance captatori informatici del tipo Trojan, capaci di attivare a distanza dispositivi che tipicamente seguono i soggetti intercettati in tutti i loro spostamenti (smartphone, tablet, computer, Apple watch...).

TROJAN DIVENTA STRUMENTO DI INDAGINE PENALE

- Il Senato, con l'approvazione del voto di fiducia al **provvedimento Orlando di riforma della giustizia penale**, ha legittima il **Trojan** come strumento di indagine.

- Il **Trojan** è un *malware* (*Malicius Software*) che inserito in pc o device dell'obiettivo target permette di svolgere diverse operazioni da remoto, quali controllare file ma soprattutto "intercettare" conversazioni e "registrare" immagini.

TROJAN DIVENTA STRUMENTO DI INDAGINE PENALE

La norma è stata inserita con un emendamento proprio dalla commissione giustizia del Senato, dopo la **pronuncia delle Sezioni Unite della Cassazione (dep. 1 luglio 2016, n. 26889**) che ne aveva ammesso la legittimità dell'utilizzo in luoghi di dimora privata anche non con attività criminosa in corso ma solo nei procedimenti relativi a delitti di criminalità organizzata, anche terroristica nonché quelli comunque facenti capo a un'associazione per delinquere, con esclusione del mero concorso di persone nel reato.

TROJAN DIVENTA STRUMENTO DI INDAGINE PENALE

Nell’ambito dei criteri di delega, il Parlamento ha introdotto quelli che il Governo dovrà osservare per la disciplina dell’utilizzo dei trojan come strumenti di indagine:

- è necessario il decreto autorizzativo del giudice, che deve indicare le ragioni per le quali l’utilizzo del trojan sia necessario per lo svolgimento delle indagini;

- l’attivazione del microfono deve avvenire solo in conseguenza di apposito comando inviato da remoto e non con il solo inserimento del captatore informatico, nel rispetto dei limiti stabiliti nel decreto autorizzativo del giudice;

TROJAN DIVENTA STRUMENTO DI INDAGINE PENALE

- a registrazione audio è avviata dalla polizia giudiziaria o dal personale incaricato secondo circostanze da attestare nel verbale descrittivo delle modalità di effettuazione delle operazioni;

- l'attivazione del dispositivo è sempre ammessa nel caso in cui si proceda per i delitti di criminalità e, fuori da tali casi, nei luoghi di **domicilio** solo se è in corso l'attività criminosa, nel rispetto dei requisiti previsti per le intercettazioni telefoniche;

- In caso di concreti casi di urgenza, il pubblico ministero può disporre la captazione informatica per delitti di criminalità organizzata con successiva convalida del giudice entro il termine massimo di quarantotto ore, sempre che il decreto d'urgenza dia conto delle specifiche situazioni di fatto che rendano impossibile la richiesta al giudice e delle ragioni per le quali tale specifica modalità di intercettazione sia necessaria per lo svolgimento delle indagini;

- i risultati intercettativi ottenuti possono essere utilizzati a fini di prova soltanto dei reati oggetto del provvedimento autorizzativo e possono essere utilizzati in procedimenti diversi a condizione che siano indispensabili per l'accertamento dei delitti per i quali è previsto l'arresto obbligatorio in flagranza;

- non possano essere in alcun modo conoscibili, divulgabili e pubblicabili i risultati di intercettazioni che abbiano coinvolto occasionalmente soggetti estranei ai fatti per cui si procede.

- il trasferimento delle registrazioni è effettuato soltanto verso il server della Procura in modo da garantire originalità ed integrità delle registrazioni;

- al termine della registrazione il captatore informatico viene disattivato e reso definitivamente inutilizzabile su indicazione del personale di polizia giudiziaria operante;

- devono essere utilizzati soltanto programmi informatici conformi a requisiti tecnici stabiliti con decreto ministeriale da emanarsi entro 30 giorni dalla data di entrata in vigore dei decreti legislativi di attuazione, che tenga costantemente conto dell'evoluzione tecnica al fine di garantire che tale programma si limiti ad effettuare le operazioni espressamente disposte secondo standard idonei di affidabilità tecnica, di sicurezza e di efficacia;

Il Sole 24 Ore
Giovedì 26 Ottobre 2017 - N. 289

GIUSTIZIA E SENTENZE

Processo penale. Pronta la riforma - Il testo del decreto delegato atteso domani in consiglio dei ministri per il primo esame

Intercettazioni, nodo trascrizione

Vietato l'inserimento nei «brogliacci» di materiale irrilevante per le indagini

Una procedura per garantire la riservatezza delle comunicazioni senza attentare al diritto dell'informazione. E poi un nuovo reato contro la diffusione di riprese e registrazioni fraudolente. Per la prima volta una disciplina articolata dei virus informatici con cui "infettare" computer e cellulari di persone sospette. Agevolazioni per le intercettazioni contro i reati di corruzione. I garticoli del decreto legislativo sulle intercettazioni che approda oggi in preconsiglio in vista della riunione di domani del consiglio dei ministri intervengono ad ampio raggio.

Quanto ai trojan horses, lo schema di decreto esclude limiti nel caso di indagini contro criminalità organizzata e terrorismo, mentre per gli altri reati andranno individuati anche in forma indiretta i luoghi in cui si sposterà il dispositivo mobile.

I punti chiave

LA PRIVACY

Una maggiore tutela della riservatezza delle comunicazioni dovrebbe essere assicurata dal divieto di procedere, da parte della polizia giudiziaria alla trascrizione di tutto quello che è irrilevante per indagini. Il pm può però recuperare, d'ufficio o chiamato in causa per dirimere dubbi da parte della stessa polizia, comunicazioni comunque utili come prova

IL REATO

Sanzionato con una pena massima fino a 4 anni di carcere, su querela di parte, chi diffonde riprese o registrazioni di comunicazioni altrui, compiute in maniera fraudolenta, con l'intenzione di provocare un danno alla reputazione o all'immagine. Prevista l'esimente dell'esercizio del diritto di difesa e di cronaca

I TROJAN HORSES

Disciplinato per la prima volta l'utilizzo dei virus informatici per infiltrare computer e cellulari delle persone sospette. Nessun vincolo per le indagini contro criminalità organizzata e terrorismo, necessità di indicare i luoghi di spostamento per gli altri reati. Al ministero della Giustizia definire i requisiti tecnici dei programmi

LA CORRUZIONE

Inserito nello schema di decreto anche un articolo per facilitare l'effettuazone delle intercettazioni nei procedimenti per i principali reati contro la pubblica amministrazione, dalla corruzione alla concussione, punti con almeno 5 anni di carcere: basteranno i sufficienti indizi di reato e la necessità per le indagini

http://www.quotidianodiritto.ilsole24ore.com/art/penale/2017-10-25/sulla-riforma-intercettazioni-nodo-trascrizioni-211516.php?uuid=AE4dilvC

Data Retention

Art. 132. Conservazione di dati di traffico per altre finalità

1. Dati relativi al traffico telefonico:
- conservati dal fornitore per **24 mesi dalla data della comunicazione**, per **finalità di accertamento e repressione dei reati**;

- per le medesime finalità, i **dati relativi al traffico telematico**, *esclusi* comunque i *contenuti* delle comunicazioni, sono conservati dal fornitore per **12 mesi dalla data della comunicazione**.

Data Retention

Art. 132. Conservazione di dati di traffico per altre finalità

1-bis. I dati relativi alle **chiamate senza risposta**:

- sono conservati per **30 giorni**.

Data Retention

Art. 132. Conservazione di dati di traffico per altre finalità

3. Entro termini prima indicati

- dati sono acquisiti presso il fornitore con ***decreto motivato del pubblico ministero*** anche su istanza del difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altre parti private.

Il **difensore** dell'imputato o della persona sottoposta alle indagini può richiedere, ***direttamente*** al fornitore i dati relativi alle utenze intestate al proprio assistito **con le modalità indicate dall'articolo 391-quater cpp** (*Richiesta di documentazione alla pubblica amministrazione*) [...].

Data Retention

Art. 132. Conservazione di dati di traffico per altre finalità

4-*ter*. Il Ministro dell'interno (o, su delega, Polizia di Stato, Carabinieri e Finanza), possono ordinare:

- ai fornitori e agli operatori di servizi informatici o telematici di conservare e proteggere, secondo le modalità indicate e per un periodo ***non superiore a 90 giorni*****,** i dati relativi al ***traffico telematico***, esclusi comunque i contenuti delle comunicazioni, **ai fini dello svolgimento delle investigazioni preventive previste** dall'articolo 226 D.Lgs. 271/89 **(Intercettazioni Telefoniche Preventive);**

- Il provvedimento, **prorogabile, per motivate esigenze, per una durata complessiva non superiore a 6 mesi,** può prevedere particolari modalità di custodia dei dati e l'eventuale indisponibilità dei dati stessi da parte dei fornitori e degli operatori di servizi informatici o telematici ovvero di terzi.

Data Retention

Art. 132. Conservazione di dati di traffico per altre finalità

4-*quater*. Il fornitore o l'operatore di servizi informatici o telematici cui è rivolto l'ordine previsto dal comma 4-ter deve:

- ottemperarvi **senza ritardo,** fornendo immediatamente all'autorità richiedente **l'assicurazione dell'adempimento.**

- **mantenere** il **segreto relativamente all'ordine ricevuto e alle attività conseguentemente svolte per il periodo indicato dall'autorità.** In caso di violazione dell'obbligo si applicano, salvo che il fatto costituisca più grave reato, le disposizioni dell'articolo 326 del codice penale **(Rivelazione ed utilizzazione di segreti di ufficio).**

Data Retention

Art. 132. Conservazione di dati di traffico per altre finalità

4-quinquies. I provvedimenti adottati ai sensi del comma 4-ter sono **comunicati per iscritto, senza ritardo e comunque entro 48 ore dalla notifica al destinatario**, al pubblico ministero del luogo di esecuzione il quale, se ne ricorrono i presupposti, li convalida. In caso di *mancata convalida, i provvedimenti assunti perdono efficacia*.

Data Retention

Art. 132. Conservazione di dati di traffico per altre finalità

5. Il trattamento dei dati per le finalità di cui al comma 1 è effettuato nel rispetto delle **misure e degli accorgimenti a garanzia dell'interessato prescritti ai sensi dell'articolo 17,** volti a garantire che i dati conservati possiedano i medesimi **requisiti di qualità, sicurezza e protezione dei dati in rete,** nonché a:

a) prevedere in ogni caso specifici sistemi di **autenticazione informatica e di autorizzazione degli incaricati del trattamento** di cui all'allegato B);

d) indicare le **modalità tecniche per la periodica distruzione dei dati,** decorsi i termini di cui al comma 1.

6 anni! E' il termine di conservazione dei dati telefonici e telematici di tutti i cittadini appena approvato alla Camera. In una direttiva sugli ascensori.

21 luglio 2017 Fulvio Sarzana Diritto penale di internet e dei nuovi media

http://fulviosarzana.nova100.ilsole24ore.com/2017/07/21/6-anni-e-il-termine-di-conservazione-dei-dati-telefonici-e-telematici-di-tutti-i-cittadini-appena-approvato-alla-camera-in-una-direttiva-sugli-ascensori/

MEDIA & REGIME

Dati personali su web e telefono, il governo dà il via alla sorveglianza di massa

di Fulvio Sarzana | 4 ottobre 2017

http://www.ilfattoquotidiano.it/2017/10/04/dati-personali-su-web-e-telefono-il-governo-da-il-via-alla-sorveglianza-di-massa/3892666/

- **Disegni di legge**
  - I DDL piu richiesti
  - Ricerca
  - Ricerca nei testi
  - Ricerca emendamenti
  - Testi dei disegni di legge
- **Leggi e decreti sul sito Parlamento**
- **Interrogazioni mozioni Sindacato ispettivo**
- **Attività non legislative**
- **Dossier di documentazione**
- **Ultimi atti pubblicati**
- **Statistiche**
- **Controllo dei rendiconti dei partiti politici**

Disegni di legge

Atto Senato n. 2886

XVII Legislatura

Segui l'iter

Dati generali | Testi ed emendamenti | Dossier | Documenti acquisiti | Trattazione in Commissione | Trattazione in consultiva | Trattazione in Assemblea | Votazioni

Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea - Legge europea 2017

Iter

10 ottobre 2017: approvato con modificazioni (trasmesso all'altro ramo)

Successione delle letture parlamentari		
C.4505	approvato	20 luglio 2017
S.2886	**approvato con modificazioni**	**10 ottobre 2017**
C.4505-B	concluso l'esame da parte della commissione	25 ottobre 2017

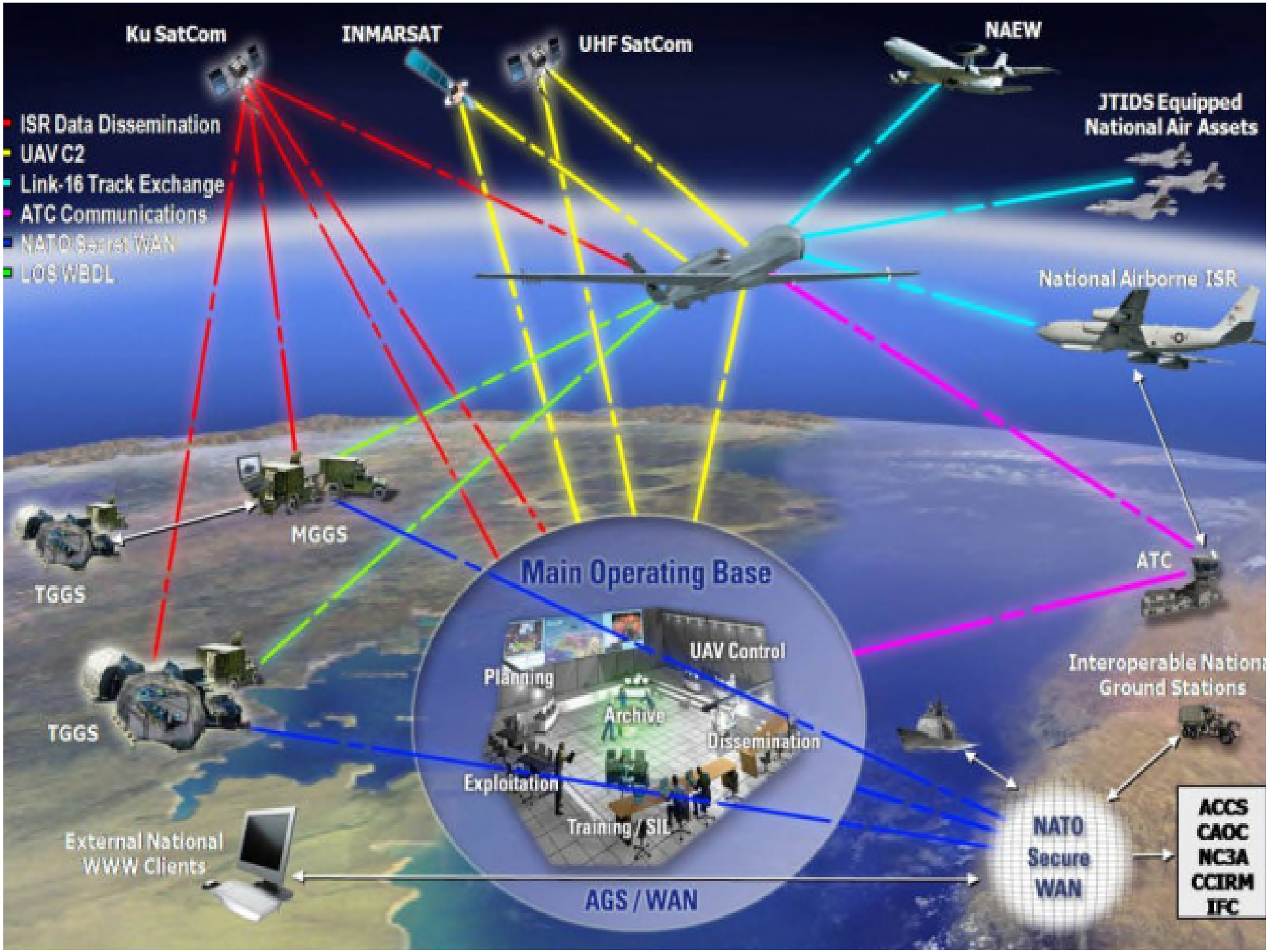
Privacy e ...cyber war

LE ARMI DEL FUTURO incontro con il generale Amos Gilad

Nella fabbrica segreta dei super droni di Israele

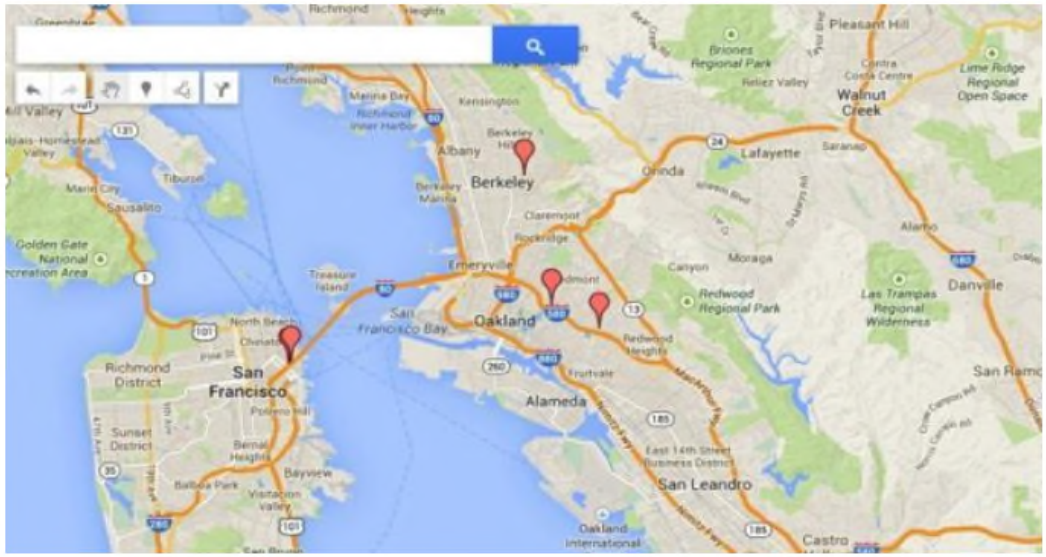
In capannoni sorvegliatissimi vicino a Tel Aviv si producono armi senza pilota. Compreso Eitan, il velivolo gigante che potrebbe distruggere le batterie iraniane

4,5


Ku SatCom
INMARSAT
UHF SatCom
NAEW
JTIDS Equipped
National Air Assets
ISR Data Dissemination
UAV C2
Link-16 Track Exchange
ATC Communications
NATO Secret WAN
LOS WBDL
National Airborne ISR
MGGS
TGGS
TGGS
ATC
Main Operating Base
UAV Control
Planning
Archive
Dissemination
Exploitation
Training / SIL
Interoperable National
Ground Stations
External National
WWW Clients
AGS / WAN
NATO
Secure
WAN
ACCS
CAOC
NC3A
CCIRM
IFC

NSA e privacy: le vie dello spionaggio sono infinite

Obama promette di limitare il monitoraggio della National Security Agency ai metadati, ma il sito Ars Technica ha scoperto che anche così si possono ottenere informazioni riservate. Ecco quali



La mappa di Ars Technica con gli spostamenti rilevati utilizzando i m etadati

http://www.lastampa.it/2014/04/02/tecnologia/nsa-e-privacy-le-vie-dello-spionaggio-sono-infinite-mi3FyLGZLZTADfCq6jUy4J/pagina.html

Metadata

Prof. David Cole

Vs

Gen. Michael Hayden

R.it | Cronaca

Home | Politica | Economia | Sport | Spettacoli | Tecnologia | Motor

Interviste - Politica »

Alessandro Di Battista: "Beppe Grillo è il garante, io mi fido, vuole evitare

Tosi: "Non serve a niente, galera per chi sbaglia"

I piani della nuova Difesa: "Arruoleremo anche hacker per difendere l'Italia dalla cyberguerra"

Il generale Graziano presenta la riforma: "Una forza integrata per le sfide future, senza gelosie di corpo"

http://www.repubblica.it/cronaca/2017/03/15/news/i_piani_della_nuova_difesa_arruoleremo_anche_hacker_per_difendere_l_italia_dalla_cyberguerra_-160572422/

Pubblicato il nuovo Piano nazionale cyber

31 maggio 2017

È stata comunicata sulla Gazzetta ufficiale n. 125 del 31 maggio 2017 l'**adozione del nuovo Piano nazionale per la protezione cibernetica e la sicurezza informatica (PDF 2 MB)**.

http://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/pubblicato-il-nuovo-piano-nazionale-cyber.html

È stata comunicata sulla Gazzetta ufficiale n. 125 del 31 maggio 2017 l'adozione del nuovo **Piano nazionale per la protezione cibernetica e la sicurezza informatica**.

Il documento – adottato dal Presidente del Consiglio su deliberazione unanime del **CISR**(Comitato interministeriale per la sicurezza della Repubblica), e registrato dagli Organi di controllo – mira a sviluppare gli indirizzi strategici previsti, tra i quali si ricordano:

- il potenziamento delle capacità di difesa delle infrastrutture critiche nazionali e degli attori di rilevanza strategica per il sistema Paese;

- il miglioramento delle capacità tecnologiche, operative e di analisi degli attori istituzionali interessati;
- l'incentivazione della cooperazione tra istituzioni ed imprese nazionali;
- la promozione e diffusione della cultura della sicurezza cibernetica;
- il rafforzamento della cooperazione internazionale in materia di sicurezza cibernetica,
- ed, infine, il rafforzamento delle capacità di contrasto alle attività e contenuti illegali *on-line.*

Home » Documentazione » Normativa di riferimento » **DPCM 17 febbraio 2017**

DPCM 17 febbraio 2017

Decreto del Presidente del Consiglio dei ministri del 17 febbraio 2017 (PDF 109 kB)

Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali

(pubblicato sulla Gazzetta Ufficiale n. 87 del 13 aprile 2017)

http://www.sicurezzanazionale.gov.it/sisr.nsf/documentazione/normativa-di-riferimento/dpcm-17-febbraio-2017.html

NUOVI SCENARI

Così i robot industriali possono essere hackerati

Ricercatori italiani hanno modificato i movimenti di un braccio robotico con un attacco informatico. E hanno scoperto quanto possono essere vulnerabili le fabbriche 4.0

LEGGI ANCHE

AP

Un difetto nei chip Intel mette a rischio la sicurezza dei computer connessi alla rete

MARCO TONELLI

f 325 · G+ · in 212

CAROLA FREDIANI

Pubblicato il 04/05/2017
Ultima modifica il 04/05/2017 alle ore 18:10

I robot sono usati sempre di più nell'industria, anche per compiere azioni complesse e delicate. Dalla logistica agli imballaggi fino alle case automobilistiche, cresce la tendenza all'automazione e alla digitalizzazione delle fabbriche - quella che viene chiamata Industria 4.0.

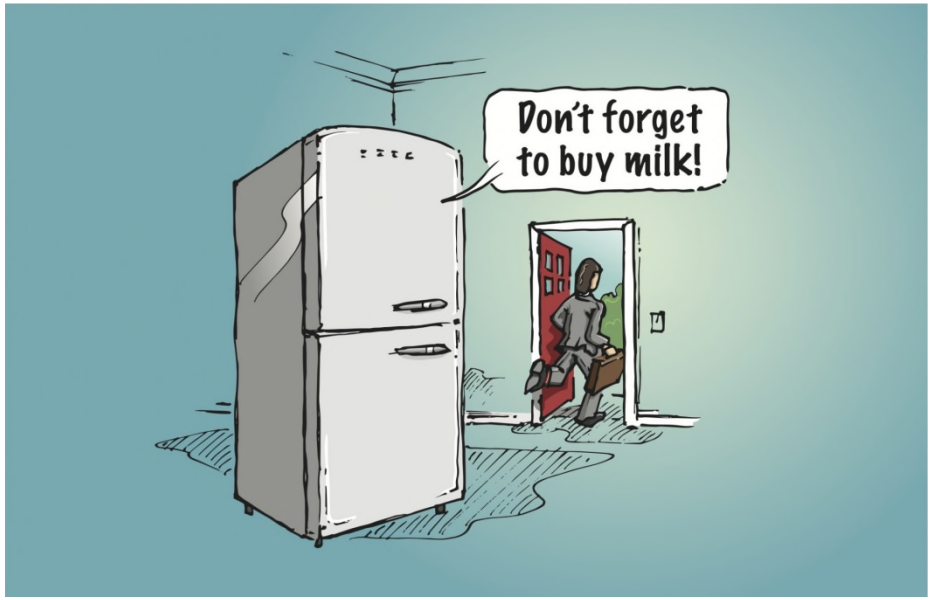
http://www.lastampa.it/2017/05/04/tecnologia/news/cos-i-robot-industriali-possono-essere-hackerati-87LOt65ts9mYBhM6dKqIxL/pagina.html

Google Perspective riconosce gli insulti online

Google ha messo a punto Perspective, delle librerie che consentono agli utenti di accedere a una rete neurale in grado di imparare a riconoscere gli insulti sul Web, al fine di censurarli.

di *Alessandro Crea* · 23 Febbraio 2017, 16:00 · (Fonte **Perspective**)

https://www.tomshw.it/google-perspective-riconosce-gli-insulti-online-83606


Don't forget
to buy milk!

HELLO
BARBIE

Sicurezza Informatica

Il fondatore dei Bitcoin (Satoshi Nakamoto) identificato dall'NSA

3 minuti necessari per leggere l'articolo

http://luca-mercatanti.com/2017/08/29/il-fondatore-dei-bitcoin-satoshi-nakamoto-identificato-dallnsa/

Utilizzando la tecnica della *stilometria*, è possibile confrontare i testi per determinare la reale fonte di un documento.

Nel corso degli anni Satoshi ha scritto migliaia di messaggi ed email e la maggior parte di questi sono pubblicamente disponibili in Rete.

L'NSA è stata in grado di utilizzare una tecnica di stilometria chiamata "**scrittore invariante**" per confrontare gli scritti di Satoshi con miliardi di "documenti campione" da persone di tutto il mondo.

Prendendo i testi di Satoshi e trovando le 50 parole più comuni, l’NSA è riuscita a creare pattern do 5.000 parole e calcolando la frequenza delle 50 principali hanno creando blocchi identificativi da 50 parole).

Il risultato è un ‘impronta digitale’ per qualsiasi cosa scritta da Satoshi che potrebbe essere facilmente confrontata con qualsiasi altra scrittura.

Ciò è avvenuto innanzitutto tramite **PRISM** (il progetto per cui NSA è autorizzata ad accedere agli account Yahoo e Google) e poi tramite **MUSCULAR** (progetto con cui l'NSA copia il traffico dati dei cavi a fibra ottica che trasportano le informazioni tra i datacenter di Google, Yahoo, Amazon e Facebook).

Si capisce facilmente come l'NSA è stata in grado di confrontare miliardi di testi con gli scritti di Satoshi per trovare la sua vera identità.

Lo sforzo è durato meno di un mese e ha portato a una partita positiva. Pare infatti che siano stati individuati una serie di soggetti identificabili come Satoshi Nakamoto, anche se sulla questione vi è ancora assoluto riserbo.

(TS//SI//NF) PRISM Collection Details

Current Providers

- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

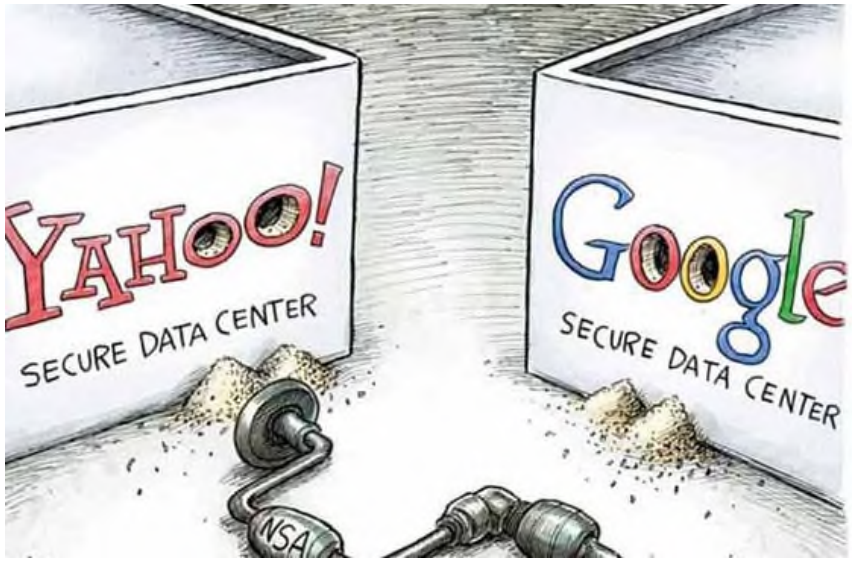
What Will You Receive in Collection (Surveillance and Stored Comms)? It varies by provider. In general:

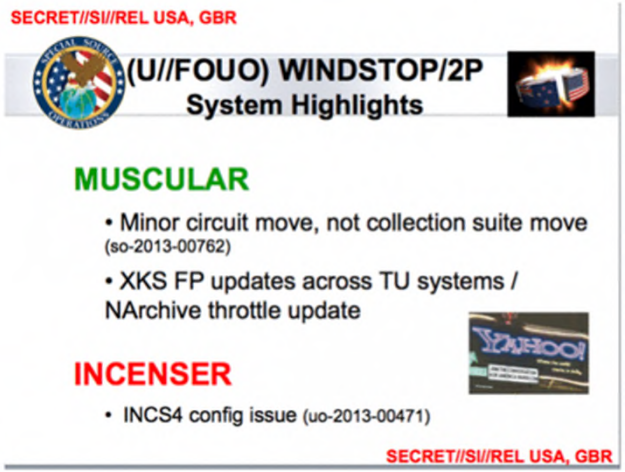
- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- **Special Requests**

Complete list and details on PRISM web page:
Go PRISMFAA

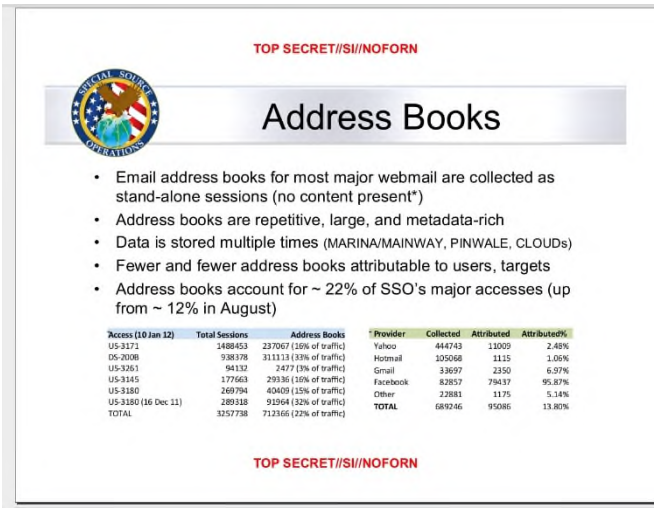
Muscular...se cerchi su google immagini

Ma in realtà…


YAHOO!
SECURE DATA CENTER
Google
SECURE DATA CENTER
NSA

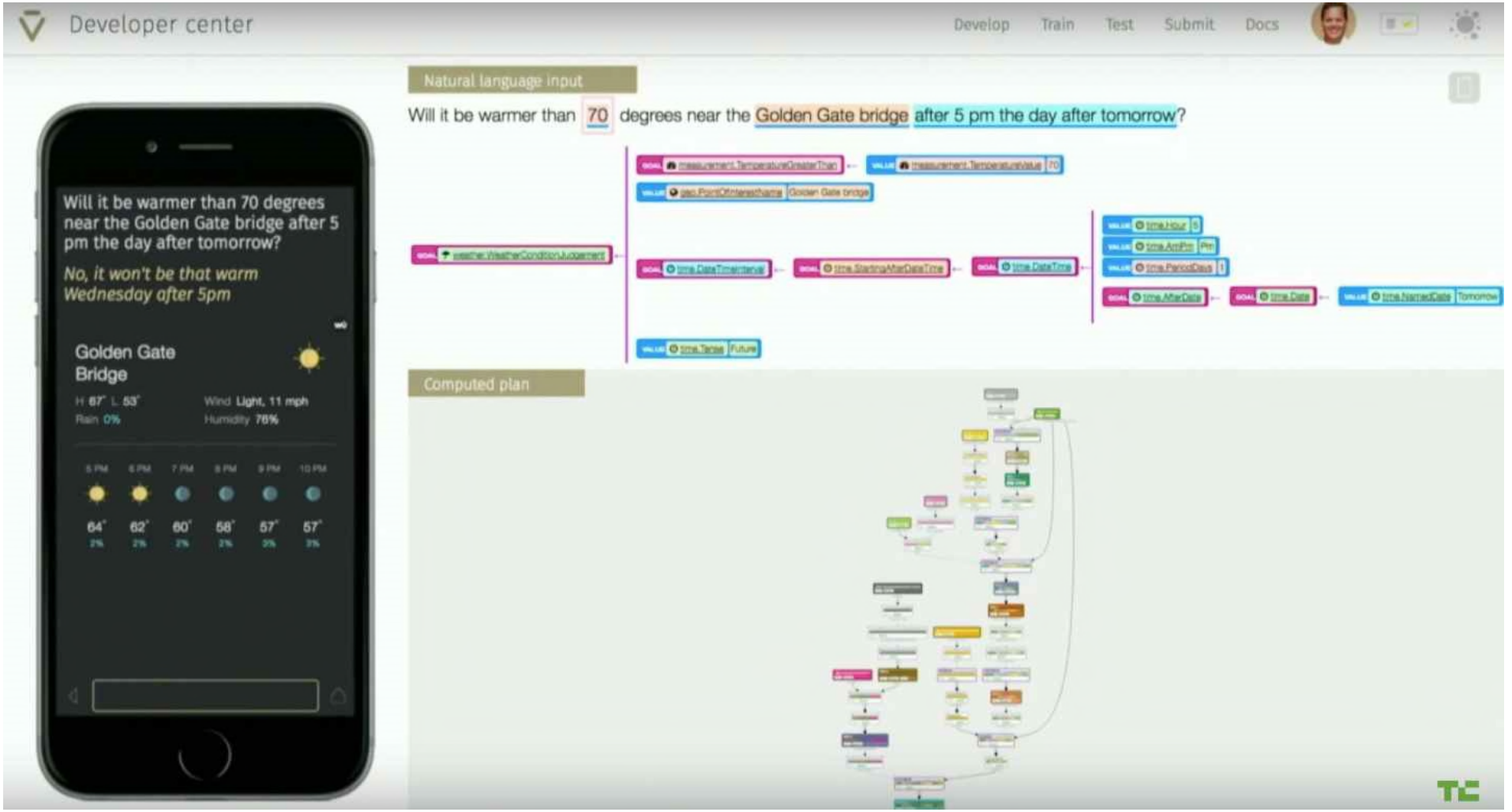

SECRET//SI//REL USA, GBR
(U//FOUO) WINDSTOP/2P
System Highlights
MUSCULAR
• Minor circuit move, not collection suite move (so-2013-00762)
• XKS FP updates across TU systems / NArchive throttle update
INCENSER
• INCS4 config issue (uo-2013-00471)
SECRET//SI//REL USA, GBR

USA TODAY
Report: NSA muscles in on Google, Yaho
Alistair Barr, USA TODAY
Program called MUSCULAR collects vast amounts of information.
SHARE
SAN FRANCISCO – The National Security Agency secretly collects information that flows between the data centers of technology giants Yahoo and Google, the Washington Post reported Wednesday, citing documents from former NSA contractor Edward Snowden and interviews with knowledgeable officials


TOP SECRET//SI//NOFORN
Address Books
• Email address books for most major webmail are collected as stand-alone sessions (no content present*)
• Address books are repetitive, large, and metadata-rich
• Data is stored multiple times (MARINA/MAINWAY, PINWALE, CLOUDs)
• Fewer and fewer address books attributable to users, targets
• Address books account for ~ 22% of SSO's major accesses (up from ~ 12% in August)
Access (10 Jan 12) Total Sessions Address Books
US-3171 1488453 237067 (16% of traffic)
DS-2008 938378 311113 (33% of traffic)
US-3261 94132 2477 (3% of traffic)
US-3145 177663 29336 (16% of traffic)
US-3180 269794 40409 (15% of traffic)
US-3180 (16 Dec 11) 289318 91964 (32% of traffic)
TOTAL 3257738 712366 (22% of traffic)
Provider Collected Attributed Attributed%
Yahoo 444743 11009 2.48%
Hotmail 105068 1115 1.06%
Gmail 33697 2350 6.97%
Facebook 82857 79437 95.87%
Other 22881 1175 5.14%
TOTAL 689246 95086 13.80%
TOP SECRET//SI//NOFORN

TRANSATLANTIC TRADE AND INVESTMENT PARTNERSHIP

VIV
THE GLOBAL BRAIN


Developer center
Develop
Train
Test
Submit
Docs
Natural language input
Will it be warmer than 70 degrees near the Golden Gate bridge after 5 pm the day after tomorrow?
Will it be warmer than 70 degrees near the Golden Gate bridge after 5 pm the day after tomorrow?
No, it won't be that warm Wednesday after 5pm
Golden Gate Bridge
H 67° L 53°
Wind Light, 11 mph
Rain 0%
Humidity 76%
5 PM 6 PM 7 PM 8 PM 9 PM 10 PM
64° 62° 60° 58° 57° 57°
Computed plan

In the digital age, gleaning the genetic information of others has become much easier than most consumers of genetic testing services realize. Going beyond the classic hacking case, in which criminals access sensitive data accompanied by identifying information, even information formerly thought to be anonymous has proven penetrable by third parties. In an article in Science, a group of researchers from the Whitehead Institute of Biomedical Research at M.I.T. demonstrated how they had been able to discover the identities of randomly selected people based on online anonymous genetic information collected as part of a voluntary study. The researchers revealed that they had been able to uncover the identities of individuals within entire families, eventually exposing the identities of nearly fifty people, including relatives who had not taken part in the study. Similarly, other researchers have discovered through their work that RNA expression can be used not only to identify an individual but also to uncover other information about the person, such as weight, diabetic profile, and HIV status. This ease of access to digital genetic information holds dire implications for incidences of genetic discrimination within the employment context.

Implications For Employment Discrimination

In the age of Big Data, and the "black box" characteristics of its accompanying algorithmic processes, there is legitimate concern that the behaviors, activities, demographic and genetic information of workers collected at the workplace-even if not used directly by the employers collecting it-could become part of datasets that ultimately are used to make employment-related decisions. As so much of the activity behind internet-scraping and machine-learning is not known-or knowable-to the people designing the programs, it is not always foreseeable that a certain algorithm will access and deploy prohibited information in its decision-making processes.

My recommendation is that employers should take seriously the worker privacy and employment discrimination concerns raised by big data and worker surveillance, and take steps to minimize the risks posed to their workers.

AMMINISTRATIVO - NUOVE TECNOLOGIE

Diritto di accesso all'algoritmo, TAR Lazio apre nuovi scenari

TAR, Lazio-Roma, sez. III bis, sentenza 22/03/2017 n° 3769

di Michele Iaselli

Pubblicato il

Archivia in cartella | Scrivi Nota | A-

*Deve essere riconosciuto il diritto di accesso all'algoritmo del software di gestione di un procedimento amministrativo ogni qualvolta quest'ultimo possa configurarsi come atto amministrativo cd. informatico in senso stretto ai fini che interessano della sua piena ammissibilità in sede di accesso agli atti ai sensi dell'**art. 22 della legge n. 241 del 1990**.*

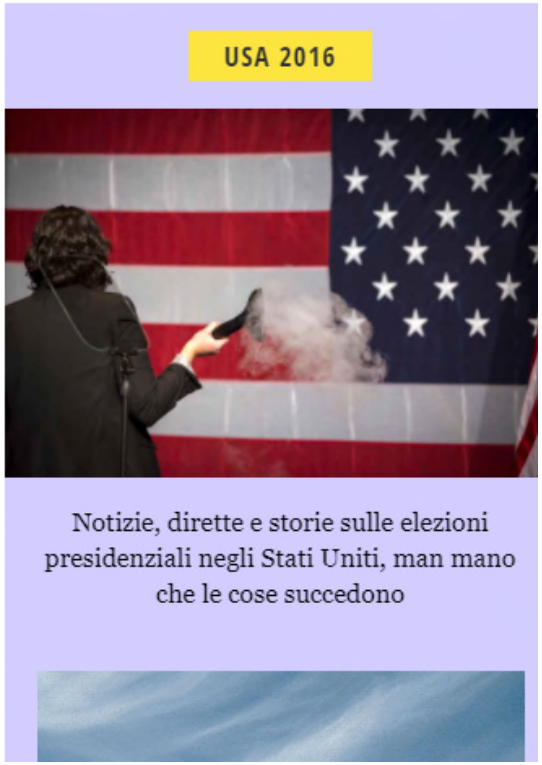
http://www.altalex.com/documents/news/2017/05/17/diritto-di-accesso-algoritmo

Trump ha vinto grazie a Facebook?

di ***Emanuele Menietti*** – ***@emenietti***

Se lo stanno chiedendo in molti, discutendo del ruolo del social network nella grande diffusione di notizie false – soprattutto su Hillary Clinton – durante la campagna elettorale

(Eduardo Munoz Alvarez/Getty Images)



http://www.ilpost.it/2016/11/11/trump-ha-vinto-grazie-a-facebook/

VINCERÀ TRUMP. LO DICE L'ALGORITMO CHE DAL 1912 NON SBAGLIA "QUASI" MAI

da Emanuele Sabatino | Nov 8, 2016 | 0 commenti

http://www.iogiocopulito.it/vincera-trump-lo-dice-lalgoritmo-che-dal-1912-non-sbaglia-quasi-mai/

LO STUDIO

I «like» su Facebook raccontano la personalità meglio degli amici

Lo studio pubblicato su Pnas ha analizzato 86.000 profili rivelando che solo il coniuge può rivaleggiare con il computer per i tratti psicologici di una persona

Computer meglio di amici e familiari nel giudicare la nostra personalità. E ad aiutarli a svelare in modo preciso elementi chiave del carattere delle persone sono speciali tracce digitali: i «mi piace» su Facebook. È quanto emerge da un nuovo studio, pubblicato su «Pnas», che confronta la capacità di computer ed esseri umani di esprimere giudizi precisi sulla nostra personalità. I giudizi delle persone si basavano sulla familiarità con l'individuo giudicato, mentre il computer usava i «like» sul social network.

Computer più bravo di amici e familiari

I risultati non lasciano dubbi: estraendo i «mi piace» disseminati in un profilo Facebook, il modello computerizzato si è rivelato in grado di svelare la personalità di un individuo in modo più accurato rispetto alla maggior parte di amici e familiari. E se lo psico-computer aveva abbastanza «like» da analizzare, solo un marito o una moglie sono risultati più abili nel descrivere con precisione di ampi tratti psicologici di un soggetto.

http://www.corriere.it/salute/neuroscienze/15_gennaio_13/i-like-facebook-raccontano-personalita-meglio-amici-a579a048-9b03-11e4-bf95-3f0a8339dd35.shtml

PNAS PNAS

Private traits and attributes are predictable from digital records of human behavior

Michal Kosinski[a,1], David Stillwell[a], and Thore Graepel[b]

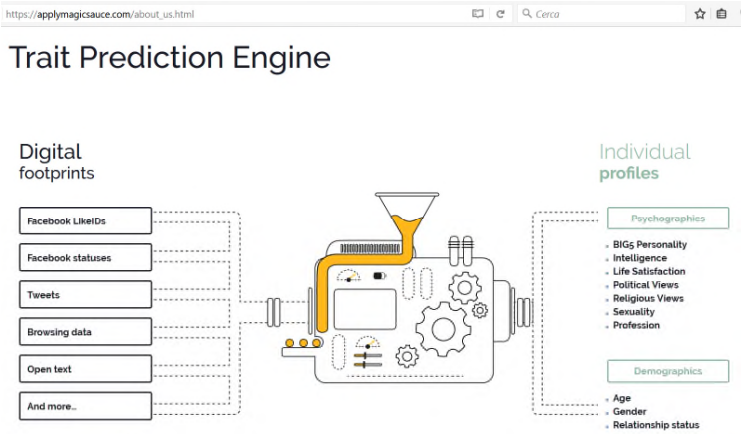
[a]Free School Lane, The Psychometrics Centre, University of Cambridge, Cambridge CB2 3RQ United Kingdom; and [b]Microsoft Research, Cambridge CB1 2FB, United Kingdom

Edited by Kenneth Wachter, University of California, Berkeley, CA, and approved February 12, 2013 (received for review October 29, 2012)

We show that easily accessible digital records of behavior, Facebook Likes, can be used to automatically and accurately predict a range of highly sensitive personal attributes including: sexual orientation, ethnicity, religious and political views, personality traits, intelligence, happiness, use of addictive substances, parental separation, age, and gender. The analysis presented is based on a dataset of over 58,000 volunteers who provided their Facebook Likes, detailed demographic profiles, and the results of several psychometric tests. The proposed model uses dimensionality reduction for preprocessing the Likes data, which are then entered into logistic/linear regression to predict individual psychodemographic profiles from Likes. The model correctly discriminates between homosexual and heterosexual men in 88% of cases, African Americans and Caucasian Americans in 95% of cases, and between Democrat and Republican in 85% of cases. For the personality trait "Openness," prediction accuracy is close to the test–retest accuracy of a standard personality test. We give examples of associations between attributes and Likes and discuss implications for online personalization and privacy.

browsing logs (11–15). Similarly, it has been shown that personality can be predicted based on the contents of personal Web sites (16), music collections (17), properties of Facebook or Twitter profiles such as the number of friends or the density of friendship networks (18–21), or language used by their users (22). Furthermore, location within a friendship network at Facebook was shown to be predictive of sexual orientation (23).

This study demonstrates the degree to which relatively basic digital records of human behavior can be used to automatically and accurately estimate a wide range of personal attributes that people would typically assume to be private. The study is based on Facebook Likes, a mechanism used by Facebook users to express their positive association with (or "Like") online content, such as photos, friends' status updates, Facebook pages of products, sports, musicians, books, restaurants, or popular Web sites. Likes represent a very generic class of digital records, similar to Web search queries, Web browsing histories, and credit card purchases. For example, observing users' Likes related to music provides similar information to observing records of songs listened to online, songs and artists searched for using a Web search en-



http://www.pnas.org/content/110/15/5802

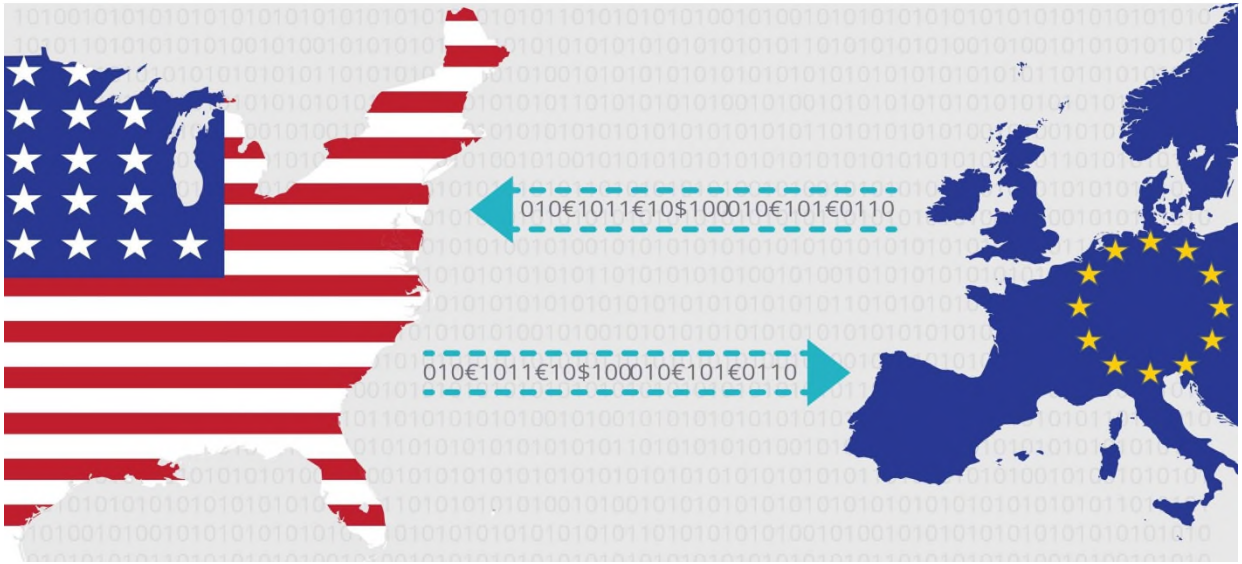
Il movimento per la **responsabilità algoritmica**

A partire dal 2013 il *Governing Algorithms*, tenutosi alla New York University, costituito da una comunità di studiosi e attivisti coalizzati per analizzare i risultati dei processi algoritmici sta spingendo verso una regolamentazione della responsabilità algoritmica.

CVRIA
COUR DE JUSTICE
DE L'UNION
EUROPÉENNE
ENTREE ERASMUS

U.S. EU
SAFE HARBOR
U.S. DEPARTMENT OF COMMERCE

Privacy Shield Framework



Nuove «identità digitali»

Sophia, ecco il primo robot al mondo a ricevere la cittadinanza

> *L'Arabia Saudita è il primo paese al mondo a concedere la cittadinanza onoraria ad un robot. Una mossa simbolica per sponsorizzare NEOM, un mega progetto futuristico da 500 miliardi di dollari.*

di **Piero Boccellato** | @pieroboccellato | 27 ottobre 2017, ore 10:10

Fonte Key4Biz – 27 ottobre 2017

Tutto chiaro … ?

Grazie per l’attenzione

Per info, chiarimenti, insulti…

sacchetto.cam@gmail.com