



# IoT, domotica e teleassistenza: questione privacy e sicurezza

**Maker Faire**  
THE EUROPEAN EDITION

**SCOPRI. INVENTA. CREA.**  
ALLA PIÙ GRANDE FIERA DELL'INNOVAZIONE

**DISCOVER. INVENT. MAKE.**

SAPIENZA  
UNIVERSITÀ DI ROMA  
MAKERFAIREROME.EU

f Maker Faire Rome  
t #MFR15

**16 - 18  
OTTOBRE  
2015**

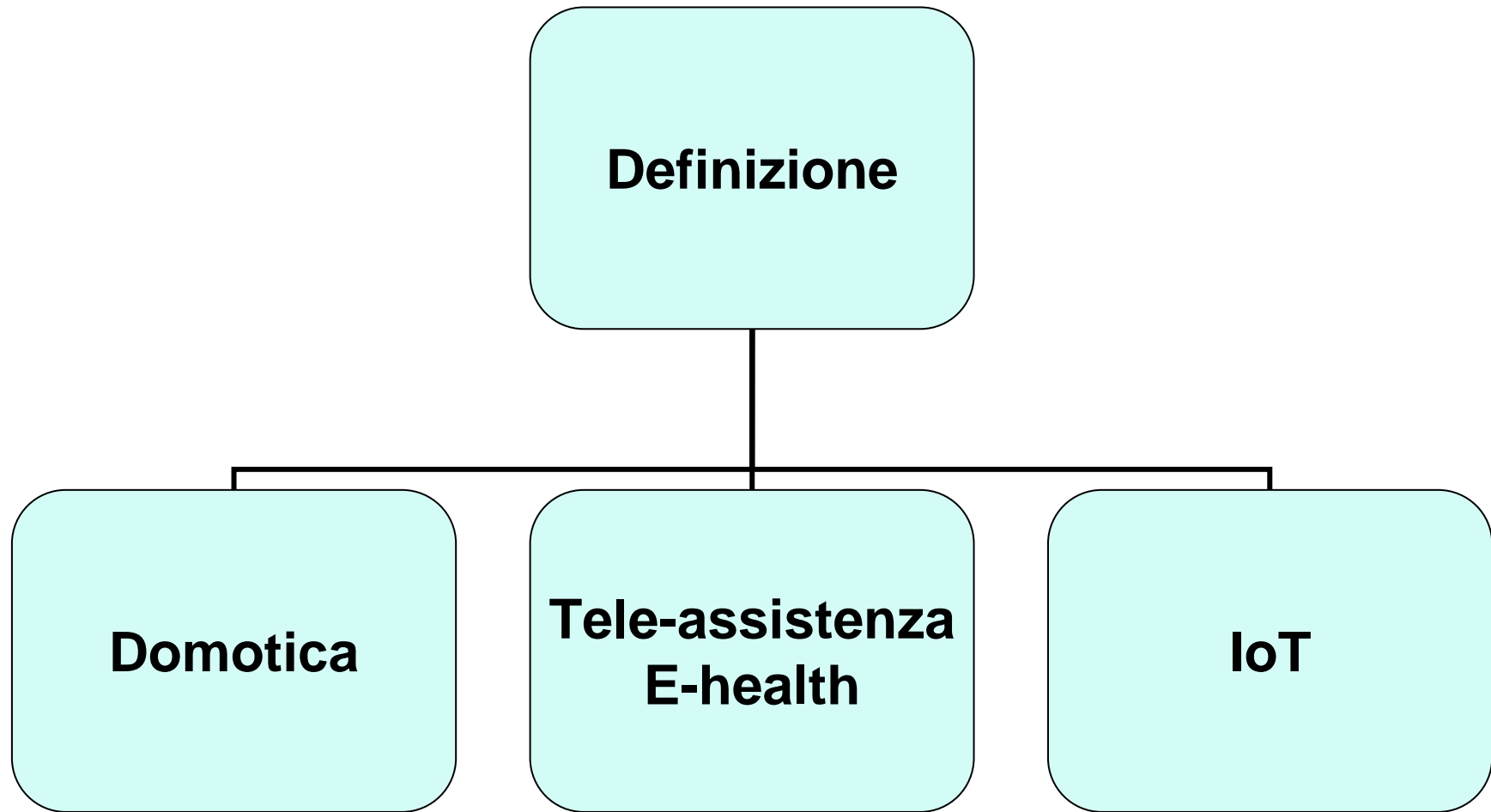
**MAKE IT HAPPEN**

Talk 126 - 16 OTTOBRE 2015 - dalle 16:15 - alle 17:15

# PREMESSA

- La Tecnologia in generale, come ogni altro strumento, non ha un valore predefinito assoluto. Spesso è l'USO che se ne fa, a determinare se sia buona o cattiva ...

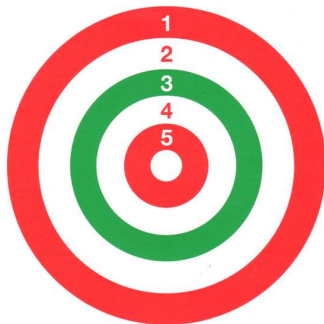




# DOMOTICA

informatique

Dal greco :Domos + informatica  
titemi ( ordinare )



Migliorare la qualità della vita  
all'interno della casa  
+ risp energetico, sicurezza, automaz. ecc

```
graph TD; Domotica[Domotica] --- Classica["Classica  
(dagli anni '60)"]; Domotica --- Moderna["Moderna  
(con internet)"]
```

Domotica

Classica  
( dagli anni '60 )

“Moderna”  
( con internet )

# Chi vive all'interno della casa?

... ingegneri ?



**gli  
ingegneri  
non  
vivono,  
funzionano!**

O persone ?



# ERGONOMIA

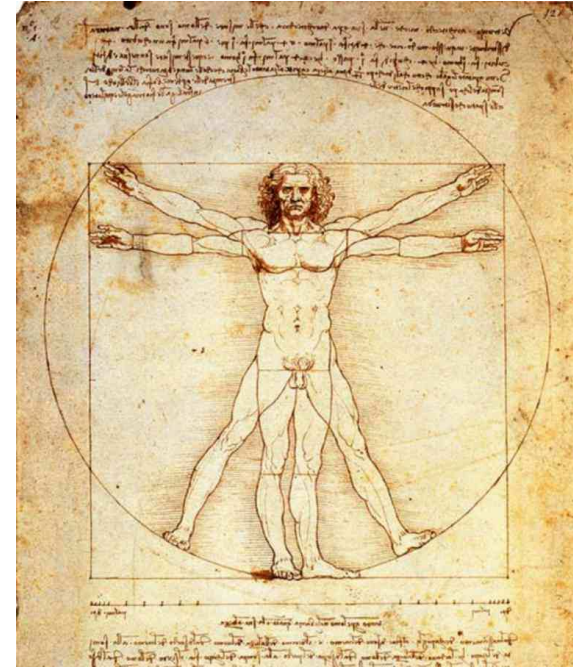
Etimologia: dal greco ergo, che significa lavoro, e nomos che significa legge, regolamento.

( L'essere umano al centro )

Interazione fra Individuo e Tecnologia con l'obiettivo di massimizzare l'utilità ed i parametri di soddisfazione

Facilità di UTILIZZO

Usabilità



# Tele-assistenza sanitaria E-health

In campo sanitario grazie alla tecnologia sviluppata

appositamente è possibile

**monitorare parametri per  
la misurazione dello stato  
di salute e per migliorare il  
benessere** quotidiano del

paziente **senza** necessità di **ospedalizzazione** ( con  
vantaggi in termini di costi, mobilità, benessere fisico  
e psicologico, reattività delle cure ecc ecc )





# IoT = Internet degli oggetti



- **Apparecchi di tutti i tipi** ( anche “solamente analogici” ) ma dotati di una parte elettronica che possa **connetterli alla rete.**
- Connessioni che servono per **controllare attuatori e leggere dati da sensori.**
- **Limiti:** cablaggi, batterie, messa a punto
- **Opportunità:** risparmio energetico, automazione, aumento qualità della vita e rendimento del lavoro
- **Rischi** correlati al SO...



# I dati = petrolio del 3° millennio

- Chi è Edward Snowden?
- Cosa è il datagate e l' NSA?
- Perché le OTT ( Over The Top ) sono un giacimento immenso di informazioni?
- Perché i dati sono così importanti, come vengono raccolti e quanto valgono?
- Cosa è la profilazione e quali i pericoli correlati?

# Edward Snowden e l' NSA

- Giovane funzionario del North Carolina che ha lavorato prima alla CIA e poi all'**NSA** e che ha rivelato al mondo “lo **spionaggio informatico**” perpetrato dal governo americano e ... per questo è accusato di alto tradimento... mentre molti lo indicano come un cavaliere della verità ...



# Datagate e NSA

- l'NSA “sembra” sia in grado di aggirare qualsiasi protocollo di protezione ( SSL, HTTPS, VPN ) e sistemi di criptazione anche più sofisticati + Backdoors  
(<http://www.newyorker.com/tech/elements/how-the-n-s-a-cracked-the-web> )
- Spiare qualsiasi movimento bancario  
(<http://www.key4biz.it/News-2013-09-16-Privacy-datagate-nsa-visa-swift-edward-snowden-der-spiegel-219803/> )
- l' NSA, in collaborazione con l'omonima agenzia inglese GCHQ, “sembra” sia in grado di copiare l'INTERO FLUSSO DATI sulle portanti ottiche che veicolano le informazioni fra i datacenter delle OTT americane della Silicon Valley ( praticamente tutte!!!! Fonte <http://www.cedmagazine.com/news/2013/10/nsa-broke-yahoo-google-data-centers>

# Datagate: danni per 35 Miliardi di \$

- Gli analisti si sono pronunciati in merito allo scandalo sull' NSA quantificando i danni per i prossimi 3 anni !!!

(<http://www.key4biz.it/News-2014-01-27-Privacy-Datagate-Nsa-Information-Technology-and-innovation-Foundation-Information-Technology-and-innovation-Foundation-222585/> )

# Mi sorge un dubbio

- Perché in così tanti si stanno impegnando nel

***“battere il mea culpa  
sul petto dell NSA”?***

... alla fine del giorno è una  
agenzia di intelligence che  
ha come obiettivo quello di  
spiare!

... sicuramente **NON TUTTO**  
e **TUTTI!**

Infatti questo sarebbe, ed è  
sbagliato!



Un particolare  
RACCAPRICCIANTE ... I ' NSA  
raggiungeva ( e raggiunge ) il suo  
obiettivo anche, semplicemente,  
accedendo ai server delle OTT ...

**allora la domanda VERA è :**  
**CHI STA SPIANDO in maniera**  
**continuativa e illimitatamente!?**



# OTT e data center

- Quanti?!...chi lo sa! Si sa solo che le superfici si misurano in ETTARI!
- Cosa fanno questi server?!  
Immagazzinano dati ... di tutti!



# Come vengono “raccolti” i dati?

- **SO Ingegnerizzati** a raccogliere ... alias: spiare ( con il consenso “spremuto” con clausole di utilizzo “sbilanciate” ...) per profilare!
- **Facebook** tramite il plug-in ( “mi piace” o altri può “seguire” e raccogliere ( illegittimamente ) i dati anche di utenti non registrati nel proprio database ([http://www.hwupgrade.it/news/web/facebook-nei-guai-in-europa-traccia-tutti-anche-gli-utenti-che-non-usano-il-servizio\\_56796.html](http://www.hwupgrade.it/news/web/facebook-nei-guai-in-europa-traccia-tutti-anche-gli-utenti-che-non-usano-il-servizio_56796.html))
- **Microsoft** può accedere a tutti gli account di posta degli utenti ([http://www.corrierecomunicazioni.it/it-world/26612\\_microsoft-ammette-possiamo-spiare-le-e-mail-degli-utenti.htm](http://www.corrierecomunicazioni.it/it-world/26612_microsoft-ammette-possiamo-spiare-le-e-mail-degli-utenti.htm) )
- **Apple** colleziona la posizione attraverso i suoi iMAC (<https://www.washingtonpost.com/news/the-switch/wp/2014/10/20/apples-mac-computers-can-automatically-collect-your-location-information/>)
- **Google** accede e scansione continuamente ed illimitatamente TUTTI i contenuti che transitano per le sue piattaforme ( da gmail ad android ) Es caso pedofilo : <http://www.lineaedp.it/news/13173/google-scova-materiale-pedopornografico-su-gmail-arrestato/> ...
- **Dati elaborati quando si utilizza Google ( disclaimer ufficiale 15 Ott 2015 )**  
**Ad esempio, quando cerchi un ristorante su Google Maps o guardi un video su YouTube, elaboriamo le informazioni relative a quella attività, che possono includere il video visualizzato, gli ID del dispositivo, gli indirizzi IP, i dati dei cookie e la posizione. I tipi di informazioni sopra descritti vengono elaborati anche quando utilizzi app o siti che ricorrono a servizi Google, come gli annunci, Analytics e il video player di YouTube.**
- **Illusione della criptazione end-to-end** (chiave e algoritmo in chiaro x G )  
I furbetti del pianetino includono anche **Amazon, Twiter** ecc ecc

# Perché i dati sono così importanti e quanto valgono?

- La **conoscenza** è il primo **vantaggio competitivo** per primeggiare!

Ma quando è il risultato dello **spionaggio**, è solamente **CONCORRENZA SLEALE!**

**Facebook acquistò whatsapp per 19 miliardi di Dollari....ecco il valore dei dati!!!**

450M x \$6 mese = circa 2,8M quindi 7 mesi bep.

[\(http://www.computarte.it/artetecnologica/2014/02/24/facebook-compra-whatsup-per-19-miliardi-di-dollari-pochi-o-troppi/ \)](http://www.computarte.it/artetecnologica/2014/02/24/facebook-compra-whatsup-per-19-miliardi-di-dollari-pochi-o-troppi/)

# Quando si possono esportare i dati extra EU?

- trasferimento di dati personali all'estero, che può aver luogo solo qualora il paese di destinazione dei dati garantisca *“un livello di protezione adeguato”* (art. 25, primo comma, direttiva 95/46/CE).

# Schrems VS Facebook

- **Maximillian Schrems** ( cittadino austriaco ) chiede a **Facebook** di cancellare tutti i dati raccolti su di lui.
- Facebook NEGA!

**ACCUSA:** Schrems adisce l'**Authorit  Irlandese di protezione dei dati personali** (ove ha sede la filiale europea di Facebook Inc.), **per contestare che i propri dati, trasferiti e trattati dall'azienda titolare dell'omonimo social network, potessero considerarsi adeguatamente tutelati dalla sorveglianza svolta dalle autorit  pubbliche degli Stati Uniti**

## **Accusa rigettata dal garante :**

L'Autorithy Irlandese respinge la denuncia dell'attivista austriaco, sulla base del presupposto che **l'adeguatezza della protezione offerta dagli Stati Uniti ai dati personali riferiti a cittadini europei e trasferiti verso aziende aderenti al "Safe Harbor" era gi  stata accertata e statuita dalla Commissione Europea, con la Decisione 2000/520/CE, venendo a configurare, di fatto, un principio gi  "assodato".**

- **Schrems si rivolge alla Corte di Giustizia Europea.**  
Qui, grazie all'appoggio dell'avvocato generale della CGE, Yves Bot,   riuscito a far dichiarare il Safe Harbor pericoloso. (<http://www.digitalic.it/wp/mercato-2/business/unione-europea-stop-al-trasferimento-di-dati-verso-gli-usa/92739> )
- **LA COMMISSIONE DA RAGIONE A SCHREMS:**sottolineando con forza la missione garantista di cui sono investite le autorit  nazionali di controllo **in virt  della Carta fondamentale dei diritti dell'Unione**

# COLPO DI SCENA: SAFE ARBOR ...NOT VALID!

## Divieto export dati perché il porto NON è sicuro!

- Martedì 6 ottobre 2015, con una clamorosa sentenza (<http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=142370>) resa nell'ambito della causa C-362/14, **la Corte di Giustizia dell'Unione Europea ha dichiarato invalida la decisione n. 2000/520/CE con cui la Commissione Europea ha aderito al programma c.d. "Safe Harbor"**, costituito da una serie di principi redatti dal Dipartimento del Commercio USA in accordo con la Commissione medesima, finalizzati a **garantire un livello adeguato di protezione dei dati personali trasferiti da persone o enti residenti in Europa alle imprese statunitensi aderenti al programma.** ([http://www.digital4.biz/digital4/nubi-grigie-sulla-tutela-dei-nostri-dati-personali-si-apre-il-caso-safe-harbor\\_43672156191.htm](http://www.digital4.biz/digital4/nubi-grigie-sulla-tutela-dei-nostri-dati-personali-si-apre-il-caso-safe-harbor_43672156191.htm))
- In riferimento al **Safe Harbor, la Corte giunge a decretarne l'invalidità** sulla base delle seguenti considerazioni:
- In primo luogo, nell'emanare una decisione di adeguatezza, la Commissione è chiamata a valutare **se il paese destinatario** del trasferimento sia **in grado di offrire** ai dati personali ricevuti un livello di **tutela e protezione**, se non identico, quantomeno "*sostanzialmente equivalente*" a quello offerto dall'ordinamento giuridico comunitario
- **Safe Harbour** trova applicazione nei confronti delle sole aziende che annualmente decidano di aderirvi **volontariamente**, non vincolando in alcun modo le autorità pubbliche statunitensi.
- **Safe Harbour è sbilanciato a favore degli USA:** ai sensi del quarto comma, dell'allegato I della Decisione 2000/520/CE, l'applicabilità dei principi "*Safe Harbor*" può essere legittimamente **limitata o sospesa** nella misura necessaria a soddisfare esigenze afferenti alla **sicurezza nazionale**, al pubblico interesse e all'osservanza delle leggi statunitensi; esigenze destinate, quindi, sempre a prevalere in ipotesi di potenziale conflitto con i principi dell'"*approdo sicuro*".
- **LA LEGISLAZIONE USA** *permetta alle autorità pubbliche di avere accesso in modo generalizzato ai contenuti di comunicazioni elettroniche deve essere considerata come una compromissione dell'essenza del diritto fondamentale del rispetto della vita privata. Allo stesso modo, una legislazione che non preveda alcuna possibilità per il singolo di esperire rimedi giuridici al fine di avere accesso ai dati personali che lo riguardano, o per ottenerne la rettifica o la cancellazione, non rispetta l'essenza del diritto fondamentale ad una tutela giurisdizionale effettiva*".
- **QUINDI:** Per tali motivi, la Corte conclude affermando che l'art. 25, comma sesto della direttiva 95/45/CE, letto alla luce degli artt. 7,8 e 47 della Carta dei diritti fondamentali dell'Unione Europea, deve essere interpretato nel senso che **una decisione adottata ai sensi di tale disposizione, come la decisione 2000/520/CE, con cui la Commissione stabilisca che un paese terzo assicura un adeguato livello di protezione, non impedisce che l'Autorità di controllo di uno Stato Membro possa esaminare la richiesta di una persona circa la tutela dei suoi diritti**, a fronte del trasferimento dei suoi dati personali all'estero, qualora sia messo in dubbio che la legislazione e la prassi del paese terzo garantiscano un adeguato livello di protezione.
- I poteri delle autorità nazionali di controllo sono stati limitati da una decisione della Commissione assunta in eccedenza rispetto alla proprie competenze e, pertanto, da considerarsi invalida.
- **l'ultima parola ritorna ai singoli Stati Membri**, che potranno esercitare la propria autorità sovrana nel decidere dove vadano conservati e trattati i dati dei propri cittadini.
- In recepimento alla direttiva europea 95/46/CE, *relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, nel sito web **garanteprivacy.it** si legge che **il trasferimento di dati personali da paesi appartenenti all'UE verso Paesi "terzi" [...] è vietato** [http://www.digital4.biz/digital4/nubi-grigie-sulla-tutela-dei-nostri-dati-personali-si-apre-il-caso-safe-harbor\\_43672156191.htm](http://www.digital4.biz/digital4/nubi-grigie-sulla-tutela-dei-nostri-dati-personali-si-apre-il-caso-safe-harbor_43672156191.htm)

# Interpretazioni restrittive della sentenza

- La conseguenza è che i Garanti Privacy Europei, d'ora in poi, **possono sospendere (non vietare a tempo indeterminato) i** trattamenti dei dati negli USA, laddove vi siano evidenze o gravi presunzioni sul fatto che i dati trattati negli USA non rispettano regole equivalenti a quelle europee.
- Tuttavia se un Garante non apre un caso a seguito del quale viene ordinata una sospensione, il trattamento si presume lecito e può continuare. **Non vi è alcun divieto preventivo** e, in questo senso, non cambia nulla. I trasferimenti possono dunque continuare.
- Inoltre, vi è da dire che le **società multinazionali possono avvalersi di policy intra-gruppo vincolanti, non toccate dalla sentenza, che, una volta approvate dai Garanti**, certificano la correttezza dei trasferimenti tra società del Gruppo (Binding Corporate Rules). ([http://www.agendadigitale.eu/identita-digitale/privacy-che-cosa-cambia-e-che-cosa-no-dopo-la-sentenza-facebook\\_1724.htm](http://www.agendadigitale.eu/identita-digitale/privacy-che-cosa-cambia-e-che-cosa-no-dopo-la-sentenza-facebook_1724.htm))

# SMARTphone = spia ( SO )

## Twitter

## Google Market

## Viber





# Indossabili ( SO )

- Raccolta dati intimi sullo stato di salute e sulle abitudini dinamiche e di alimentazione : pericolo profilazione sanitaria  
[http://www.wirelessweek.com/news/2014/08/fitbit-denies-claims-it-sells-personal-data?et\\_cid=4116888&et\\_rid=575253763&type=cta](http://www.wirelessweek.com/news/2014/08/fitbit-denies-claims-it-sells-personal-data?et_cid=4116888&et_rid=575253763&type=cta)



# La nuova frontiera dello spionaggio continuativo ed invasivo è la tecnologia dello **Speech to text** (**Siri, Google Now, Cortana ecc. )**

- Quando i suoni vengono trasformati in segni con significato compiuto come le parole, ad analizzare il tutto ci pensano gli algoritmi semantici ingegnerizzati su schemi di intelligenza artificiale...

Potenzialmente **tutte le nostre conversazioni**, in **presenza di un microfono collegato in rete, possono essere trascritte, interpretate , USATE, immagazzinate e rivendute...** proprio come nel caso di elettrodomestici SPIE

<http://www.techeconomy.it/2014/04/09/internet-of-things-gli-elettrodomestici-violeranno-nostra-privacy/>

# Spionaggio SMART TV ( SO )

- Una SMART-tv è uno SMART-phone con un grande schermo!
- Most smart TVs are harvesting plenty of data on top of that, including viewing habits, search terms, browsing history... pretty much anything that makes a TV "smart" is collected and transmitted ***not just to the manufacturer, but to plenty of unknown third parties.***
- Class action contro LG (<http://www.ecommercetimes.com/story/79491.html>)
- Class action vs Samsung  
(<https://www.techdirt.com/articles/20150206/04532329928/samsungs-smart-tvs-are-collecting-storing-your-private-conversations.shtml>)
- <http://www.internetontrial.com/privacy-law/do-you-control-your-smart-tv-using-voice-commands/>
- <http://www.nyrealestatelawblog.com/Manhattan-Litigation-Blog/2013/August/YOUR-TV-IS-WATCHING-YOU-.aspx>

# LG smart TV ( OS ) ascolta...

- In LG's [50+ pages of smart TV fine print](#), it says the following about voice recognition: ***I agree that LG Electronics Inc. ("LGE") may process Voice Information in the manner set out in the Privacy Policy and below.***

*Voice Information refers to the recording of voice commands and associated data, such as information about the input device that is used to record commands (e.g., Magic Remote or built-in microphone), OS information, TV model information, content provider, channel information and service results.*

***I understand and agree that Voice Information may be use for the purpose of powering the voice activation feature when used to control, receive, and improve LG Smart TV Services and as described in the Privacy Policy.***

***I further understand and agree that LGE may share Voice Information with third parties, including providers of voice analytics.***

***I understand and agree that Voice Information may be transferred to, and used by, third party service providers on LGE's behalf in various countries around the world (including Korea), some of which may not offer the same level of data protection, for the purposes set out in the Privacy Policy.***

# SAMSUNG SMART TV ( OS) ascolta...

- [Samsung's privacy policy says this](#): *To provide you the Voice Recognition feature, some voice commands may be transmitted (along with information about your device, including device identifiers) to a third-party service that converts speech to text or to the extent necessary to provide the Voice Recognition features to you. In addition, **Samsung may collect and your device may capture voice commands and associated texts** so that we can provide you with Voice Recognition features and evaluate and improve the features. **Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition.***
- . (<http://www.mouseprint.org/2015/02/16/shussh-dont-say-that-in-front-of-the-kids-smart-tv/> )
- <http://arstechnica.com/tech-policy/2015/02/privacy-advocate-tells-ftc-that-samsung-smart-tvs-are-deceptive/>

# Cosa è la profilazione e quali i pericoli correlati?

- PARADOSSO: Quando i dati ci dipingono dinamicamente in un filmato continuo come nemmeno noi riusciremmo a fare anche solo puntualmente guardandoci allo specchio.
- Locazione spazio-tempo.
- **Riconoscimento vocale e facciale**
- Foto
- Incrocio dei dati personali

# Lo studio del Prof. Christoph Sorge Saarland University ( Germania )

- Uno studio completo di come , intercettando e “sniffando” i dati delle comunicazioni Wi-fi fra i sensori e gli attuatori all’interno della casa sia possibile conoscere con molta accuratezza il tipo di impianto, i sensori , gli attuatori, l’utilizzo fatto e ... la presenza all’interno della casa.
- Anche le comunicazione criptate sono analizzate sulla base del periodo di refresh del segnale per desumere la presenza dell’utente. ( possibile rimedio dummy trafic ).

# Privacy e sicurezza sono ancora trascurabili?!

- Istallereste a casa tecnologia che vi potrebbe “tradire” in qualsiasi momento (SO ed hw ingegnerizzato a tale scopo)!?

Conoscere per saper scegliere e Cartesio come angelo custode!





# Scelta della Tecnologia rispettosa della privacy

Spionaggio e infrazione Privacy

Nido da proteggere





Comput**Arte**®: quando la tecnologia si veste d'Arte, rispetta e protegge la tua privacy ©.

**VPC = Very Personal Computer**

La presentazione con tutti i collegamenti saranno disponibili su [www.computarte.it](http://www.computarte.it)

Dr. Vasco Petruzzi

info@computarte.it