Convegno Annuale AISIS

eHealth 2020

IOT E BIG DATA
e Regolamento UE 679/2016

avv. silvia stefanelli

Cagliari, 13 e 14 ottobre 2016

Convenzione diritti Uomo – art. 8
(4 dicembre 1950)

Giurisprudenza GUCE

Dir. 95/46/CEE

Atti WP 29

Provvedimenti autorità competenti

Giurisprudenza CEDU

Giurisprudenza nazionale

Regolamento UE

IOT IN AMBITO SANITARIO

telemedicina

medicina personalizzata

ricerca

Privacy: "Internet delle cose", utenti poco tutelati. Risultati dell'analisi internazionale per il "Privacy Sweep 2016"

Ascolta

Stampa PDF Invia per mail Condividi

SCHEDA

Doc-Web:
5443681

Data:
22/09/16

Argomenti:
Tablet , Smartphone , Dati sensibili , Dati sanitari

Tipologia:
Comunicato stampa

DOCUMENTI CITATI

"Internet delle cose" sotto la lente delle Autorità garanti privacy

VEDI ANCHE (4)

Privacy: "Internet delle cose", utenti poco tutelati
I risultati dell'analisi internazionale svolta dalle Autorità garanti della privacy di 26 Paesi per il "Privacy Sweep 2016"

Su oltre trecento dispositivi elettronici connessi a Internet - come orologi e braccialetti intelligenti, contatori elettronici e termostati di ultima generazione - più del 60% non ha superato l'esame dei Garanti della privacy di 26 Paesi.

E' quanto emerge dall'indagine a tappeto ("sweep"), a carattere internazionale, avviata lo scorso maggio dalle Autorità per la protezione dei dati personali appartenenti al Global Privacy Enforcement Network (GPEN), di cui fa parte anche il Garante italiano, per verificare il rispetto della privacy nell'Internet delle cose (IoT).

I riscontri raccolti dagli esperti delle Autorità, su più di trecento apparecchi delle principali società del settore, hanno fatto emergere, a livello globale, gravi carenze nella tutela della privacy degli utenti:

- il 59% degli apparecchi non offre informazioni adeguate su come i dati personali degli interessati sono raccolti, utilizzati e comunicati a terzi;
- il 68% non fornisce appropriate informazioni sulle modalità di conservazione dei dati;
- il 72% non spiega agli utenti come cancellare i dati dal dispositivo;
- il 38% non garantisce semplici modalità di contatto ai clienti che desiderano chiarimenti in merito al rispetto della propria privacy.

Alcuni dispositivi analizzati hanno presentato anche problemi sulla sicurezza dei dati, ad esempio trasmettendo "in chiaro" (quindi in modalità non criptata) al medico curante informazioni relative alla salute degli utenti.

Leggermente migliori, ma comunque preoccupanti, i risultati delle analisi condotte dal Garante italiano sul rispetto della privacy da parte di alcune delle principali società nazionali che offrono prodotti nel settore della domotica: solo il 10% infatti non fornisce agli utenti

A.29WP Opinion 8/2014 on the Recent Developments on the Internet of Things

Wearable Computing

Quantified self

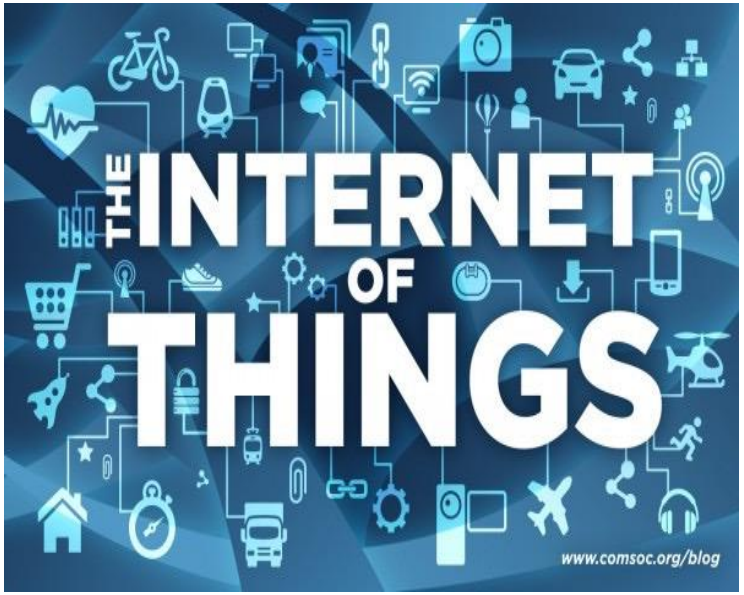
Domotics

(CON-)TITOLARE O RESPONSABILE?

PROPORZIONALITA'?

RESPONSABILITA'?

PROFILAZIONE?



INFORMATIVA?

CONSENSO?

DIRITTI SOGGETTO INTERESSATO?

TRASFERIMENTO DATI?

DATA PROTECTION BY DESIGN!

FINALITA'?

CHIARIRE I RUOLI PRIVACY

PROPORZIONALITA’

RESPONSABILITA’
DATA PROCESSING AGREEMENTS

PROFILAZIONE

THE PRIVACY OF THINGS

INFORMATIVA

CONSENSO / *LIDC*
PRIVACY BY CHOICE

TRASFERIMENTO DATI

DIRITTI SOGGETTO
INTERESSATO

PIA & DATA PROTECTION BY DESIGN

PRINCIPIO DI FINALITA’

che cosa devo tenere presente

- coinvolgimento iniziale
  per svolgere Data Protection Impact Assessment e strutturare il trattamento secondo il principio di **Data Protection by Design!**

- Identificare con esattezza:

  - flusso dei dati;
  - tipologia di dati trattati (es., sensibili);
  - i soggetti che svolgono il trattamento;
  - i ruoli privacy di tali soggetti (i.e., titolare, responsabile, con-titolare);
  - le finalità del trattamento di ogni (con-)titolare nel breve e medio/lungo termine

che cosa devo tenere presente

- Redigere informative trasparenti e comprensibili
- Raccogliere i consensi necessari
- Assicurare un effettivo esercizio dei diritti del soggetto interessato
- Notifica / Autorizzazione se necessarie
- Identificare il corretto presupposto giuridico per porre in essere trasferimenti di dati fuori dallo Spazio Economico Europe (SEE) verso paesi che non offrono un “adeguato” livello di protezione dei dati

che cosa devo tenere presente

- Porre in essere adeguate misure di sicurezza tecniche ed organizzative per proteggere I dati (NB. Rigorosa gestione delle identità e controllo degli accessi)
- Identificare e porre in essere adeguate procedure di conservazione dei dati
- Redigere solidi accordi di protezione dei dati personali/lettere di nomina a responsabile
- Non dimenticare: formazione e creazione di procedure interne

BIG DATA
in ambito sanitario

DOCUMENTI DA CONSULTARE

GRUPPO DI LAVORO 29

Opinion 4/2007 on Concept of Personal Data",
Opinion 3/2013 on "Purpose Limitation",
Opinion 5/2014 on "Anonymisation Techniques",
Opinion 6/2014 on "Legitimate interests",

Statement on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU (2014)

GARANTE EUROPEO DELLE PROTEZIONE DEI DATI

Preliminary Opinion on Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy (marzo 2014)

Opinion on Meeting the challenges of big data**:** A call for transparency, user control, data protection by design and accountability (nov 2015)

*Furthermore, w**ith the advent of the 'Internet of Things', much of the data collected and communicated by the increasing number of personal and other devices and sensors will be personal data:** the data collected by them can be easily related to the users of these devices whose behaviour they will monitor.*

These may include highly sensitive data including health information and information relating to our thinking patterns and psychological make-up.

*Opinion on Meeting the challenges of big data**:** A call for transparency, user control, data protection by design and accountability (nov 2015)*

Cosa s'intende per "big data"?

grandi serie di dati digitali spesso detenuti da società, governi e altre organizzazioni che vengono successivamente analizzati per mezzo di algoritmi informatici

Article 29 Working Party, Opinion 03/2013 on purpose limitation, p. 35. Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

BIG DATA E ANALITICS

raccolta
conservazione
analisi
utilizzo

ESTRAZIONE VALORE

com'è il dato che sto trattando?

art. 4 reg. 679/2016

. **dato personale** qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»);

si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

. **pseudonimizzazione**

il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

anonimizzazione

A29DPWP Opinion 05/2014 on Anonymisation Techniques

Adopted on 10 April 2014

consenso
art. 4 punto 11

qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

parere WP 29 n. 15 del 13 luglio 2011

.

Finalità del trattamento
interessi legittimi del titolare

I legittimi interessi di un titolare del trattamento… possono costituire una base giuridica del trattamento, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato, tenuto conto delle ***ragionevoli aspettative nutrite dall'interessato in base alla sua relazione con il titolare del trattamento.***

l'esistenza di legittimi interessi richiede un'attenta valutazione anche in merito all'eventualità che l'interessato possa ragionevolmente attendersi che abbia luogo un trattamento a tal fine.

Gli interessi e i diritti fondamentali dell'interessato potrebbero in particolare prevalere sugli interessi del titolare del trattamento qualora i dati personali siano trattati in circostanze in cui gli interessati non possano ragionevolmente attendersi un ulteriore trattamento dei dati personali.

Opinion 3/2013 on "Purpose Limitation"
Opinion 6/2014 on "Legitimate interests"

Principi generali

- Necessità e minimizzazione
- Proporzionalità
- Finalità
- *"Compatible Use"* test
- Qualità dei dati
- Sicurezza
- Trasparenza
- Accesso
- Responsabilità/Accountability

+ Informative trasparenti, facilmente accessibili e comprensibili

+ consenso ***opt-in***
- Interesse legittimo - altre basi giuridiche ex art.7 Direttiva 95/46/CE

= Trattamento lecito

*Cosa deve chiedersi il titolare?**

- *Cosa stiamo raccogliendo?*
- *Perché?*
- *Come useremo quanto raccolto?*
- *Ve n'è la necessità?*
- ***Ne trarremo le informazioni (non dati personali) di cui abbiamo bisogno?***

• LA PRESENTE E' LA TRADUZIONE DI UNA SLIDE PRESENTATA DA KATHERINE FITHEN, CHIEF PRIVACY OFFICER DI THE COCA COLA COMPANY, A BIG DATA WORLD EUROPE, 20 SETTEMBRE 2012

*Cosa chiedersi il DPO?**

- *Cosa/Perché/Come stiamo raccogliendo e trattando; e se abbiamo bisogno di tali dati eprsonali? (…)*
- ***Stiamo svolgendo un trattamento in conformità alla legge applicabile?***
- *Dove son registrati I dati? Se I dati sono trasferiti all'estero ciò avviene su un presupposto giuridico (es. clausole contrattuali tipo)?*
- *Chi può accedere ai dati?*
- *Per quanto tempo i dati vengono conservati?*
- *Vengono fornite al soggetto interessato informazioni adeguate, con particolare riferimento a alla tipologia di dati raccolti, le finalità e modalità di trattamento?*
- ***L'informativa è accessibile e comprensibile?***

• LA PRESENTE E' LA TRADUZIONE DI UNA SLIDE PRESENTATA DA KATHERINE FITHEN, CHIEF PRIVACY OFFICER DI THE COCA COLA COMPANY, A BIG DATA WORLD EUROPE, 20 SETTEMBRE 2012

Grazie dell'attenzione e buon lavoro