INTERNET OF THINGS
PROFILI LEGALI E RESPONSABILITÀ

DAS SUPSI IoT
CONFERENZA – 7 MAGGIO 2014

Avv. Gianni Cattaneo, Lugano
Cattaneo & Postizzi Studio legale SA
www.infodiritto.net
contatto@infodiritto.net

Introduzione

IoT in Swisslex

«Choc» del giurista «tradizionale»

Come superarlo?

Giurista «creativo» e «aperto»

→ UE: all'avanguardia:

- Raccomandazione 12.05 2009 Commissione
- Procedura di consultazione (2012): rapporto 16.01.2013

↗ Italia: 6 mio oggetti (+20%), mercato EUR 900 mio (+11%); centri di ricerca di eccellenza sul tema

Aspetti giuridici I

Dare un quadro legale a IoT

Opzioni:

a) Senza regole
b) Hard law
c) Autoregolamentazione
d) Soft law (co-regulation)

Aspetti giuridici I

Hard law: diritto nazionale dispositivo e/o imperativo

Vantaggi:

- «vicinanza», diritto «su misura», sovranità
- attuazione attraverso i Tribunali statali

Svantaggi:

- territorialità vs globalità del fenomeno IoT, incertezza del diritto (frammentazione e neutralità tecnologica)

Correttivi:

- Trattati internazionali (tra Stati)
- Leggi Modello Organizzazioni Internazionali (es. UNCITRAL)
- Legislatore internazionale (OMC? OCSE?)

Aspetti giuridici I

Autoregolamentazione: regole di comportamento autoimposte dai membri di un dato settore e «need-driven»

Motivazioni: (i) esigenza di ordine / norme certe; (ii) incrementare la fiducia degli utenti; (iii) indurre lo Stato a non legiferare

Vantaggi:

- efficienza (rispecchiano esigenze reali e le tecnologie in uso), flessibilità / adattabilità (rispetto all'evoluzione della tecnologia), incentivo al rispetto volontario, economicità, sanzionabilità delle violazioni (pene convenzionali, sanzioni pecuniarie, esclusione dalla comunità, perdita di reputazione)

Svantaggi:

- carattere giuridicamente non vincolante per il settore nel suo complesso, regole fatte dalla comunità per soddisfare le proprie esigenze (conflitto d'interessi)

Aspetti giuridici I

Soft law: codici di condotta esprimenti un impegno fermo di natura privata del settore interessato che si inserisce in un quadro normativo di fondo stabilito in via legislativa dallo Stato

Vantaggi

Effetto obbligatorio generale e controllo giudiziario, perlomeno quanto ai principi fissati dalla legge quadro e ai diritti di terzi; efficienza, flessibilità, adattabilità alla luce di modificate esigenze del settore / degli utenti e dell'evoluzione della tecnologia

Svantaggi

«Incertezza» (imprevedibilità), mutabilità,

Problema resta: territorialità vs globalità del fenomeno IoT

Aspetti giuridici II

La protezione della sfera privata

- IoT (animali / cose) quale strumento di autenticazione, monitoraggio e profiling degli utenti (PF e PG)
- difficoltà: «bene» apprezzato / protetto a livello globale in maniera molto variabile (vedi US vs UE/CH)
- In CH: diritto
  - costituzionale: effetto negativo verticale (non ingerenza dello Stato)
  - civile: effetto negativo orizzontale: diritto della personalità assoluto (erga omnes) e inalienabile (motivi di lesione?)
  - è privato tutto ciò che non è «pubblico»

    Sono pubblici: «gli avvenimenti e le situazioni che il soggetto accetta di condividere con persone estranee alla propria sfera di relazioni private, sia perché si svolgono pubblicamente, sia perché sono il fatto di un gruppo di persone comprendente il soggetto medesimo, sia ancora perché riguardano la sua attività pubblica» (DTF 97 II 97)
  - Motivi giustificativi della lesione: consenso, interesse pubblico o privato preponderante o legge

Aspetti giuridici II

La protezione della sfera privata

Sfide per l'IoT in questo ambito:

- esigenza di un quadro giuridico globale vs eterogeneità / differenziazione degli utenti (sensibilità, utilizzazioni ecc.)
- diritto di essere informato sull'esistenza tag / sui dati raccolti e processati
- diritto del proprietario di disattivare / controllare il tag / sensore e le informazioni ad esso collegate («silence of the chip»)
- divieti / restrizioni legali all'uso di tags in determinati ambiti o situazioni
- imposizione di standards di sicurezza IT onde impedire l'accesso alle informazioni da parte di persone non autorizzate
- promozione Privacy Enhancing Technologies (PET)
- obbligo legale / incentivi all'uso di tags in certi ambiti
- definizione di un chiaro regime di responsabilità in caso di violazione della privacy

Aspetti giuridici III

La sicurezza

- funzionamento del sistema / della piattaforma globalmente
- corretta identificazione e monitoraggio dell'oggetto
- autenticità e integrità delle informazioni correlate al tag (EPC);
- prevenzione generale dalle infezioni informatiche (e conseguenti abusi dei «pirati informatici»)
  - es. lotta contro lo spam (frigorifero), data mining, furto di dati personali, spionaggio industriale ecc.

Sfide per l'IoT in questo ambito:

- attuare globalmente adeguati standards di sicurezza IT
- supportare certe tecnologie a scapito di altre
- definizione di un chiaro regime di responsabilità e di comunicazione alle parti interessate in caso di «breach» di sicurezza

Aspetti giuridici IV

Ulteriori aspetti giuridici:

1. responsabilità dell'utilizzatore di un prodotto «smart»

   (ad esempio: frigorifero spammatore, malfunzionamento sistema di allerta di una smart car causa un incidente, violazione della privacy / dati nella domotica (immagine, profiling))

1. responsabilità degli intermediari online
2. diritto di accesso al sistema (apertura, non discriminazione, trasparenza);
3. lotta contro la concorrenza sleale e le distorsioni del mercato, nonché degli abusi nel caso di posizioni dominanti
4. tutela dell'innovazione (proprietà intellettuale: lotta alla contraffazione; es. Pfizer, RFID su Viagra dal 2006 in US)
5. eliminazione delle barriere giuridiche:
   - armonizzazione e regolamentazione delle radio frequenze a livello globale (frequenza universale per i tag RFID?)
   - armonizzazione a livello globale delle regole sulla salute pubblica relative alle radiazioni elettromagnetiche emesse dai RFID tags (inquinamento elettromagnetico)

Per gli approfondimenti:

- www.infodiritto.net

- Grazie mille per l'attenzione!