



Oracle Community For Security

Europrivacy e Data Protection alla luce della Digital Transformation, IoT e BigData

Francesca Gatti,
AUSED, Europrivacy
19 dicembre 2016, Milano



EUROPRIVACY.INFO
#READY4EUDATAP
#40ANNIAUSED
#VITEPARALLELECIO



www.europrivacy.info
nasce nel 2015 grazie ad
AUSED, CLUSIT e Oracle
Community for Security,
come osservatorio
permanente sul nuovo
Regolamento Europeo
sulla Data Protection.

The screenshot shows the homepage of the website www.europrivacy.info. At the top left is the logo, which consists of a stylized 'E' with a red and blue gradient, surrounded by blue stars, followed by the word 'PRIVACY' in blue. Below the logo is a horizontal navigation menu with the following items: HOME (highlighted in blue), BLOG, EVENTI, CONTRIBUTORI, SPONSORS, PARTECIPA, CATEGORIE, and Q&A. The main content area is titled 'Home' and features a dashed line separator. Below this, there is a section titled 'Regolamento del Parlamento Europeo e del Consiglio relativo alla Protezione delle Persone Fisiche con riguardo al Trattamento dei Dati Personali, nonché alla libera circolazione di tali dati.' This section contains two paragraphs of text: 'Il 14 Aprile 2016 il Regolamento sulla Protezione dei Dati è stato definitivamente approvato dal Parlamento Europeo.' and 'E' stato pubblicato in Gazzetta Ufficiale Europea il 4 Maggio 2016 ed è entrato in vigore il 24 Maggio 2016.' At the bottom of this section, it states 'Il Regolamento si applicherà a decorrere dal 25 maggio 2018.' To the right of the main content area, there is a sidebar with a language selector showing the UK and Italian flags. Below the language selector is a 'Login' button, followed by the text 'The registered user can login here' and 'To create an account check here'. Underneath is a 'Categorie' section with a list of categories: 'Codici di condotta e certificazione (3)', 'Violazione dei dati (21)', 'Data Protection Officer (24)', and 'Eventi (4)'. At the bottom of the page, there is a cookie consent banner that reads 'er our services. By using our services, you agree to our use of cookies. More Info | Close'. The bottom of the screenshot shows a Windows taskbar with various application icons (Internet Explorer, Microsoft Word, Adobe Reader, Firefox, PowerPoint, Outlook) and system tray icons (volume, battery at 53%, network, and system clock).

Mission 2017 – maggio 2018

- Accompagnare le aziende nel percorso di adozione del GDPR con contributi non direttamente commerciali facendo leva sulla comprovata professionalità delle nostre aziende e dei nostri membri contributori
- La specificità di Europrivacy sta nella ricchezza, nella varietà e nella libertà dei contributi che realizzano un foro precompetitivo utile sia ai fornitori che agli utenti
- 44 contributori - Chiunque può contribuire previa valutazione delle competenze nelle materie trattate dal sito.
- Nel 2017 le aziende lavorano sul GDPR: è l'anno chiave!

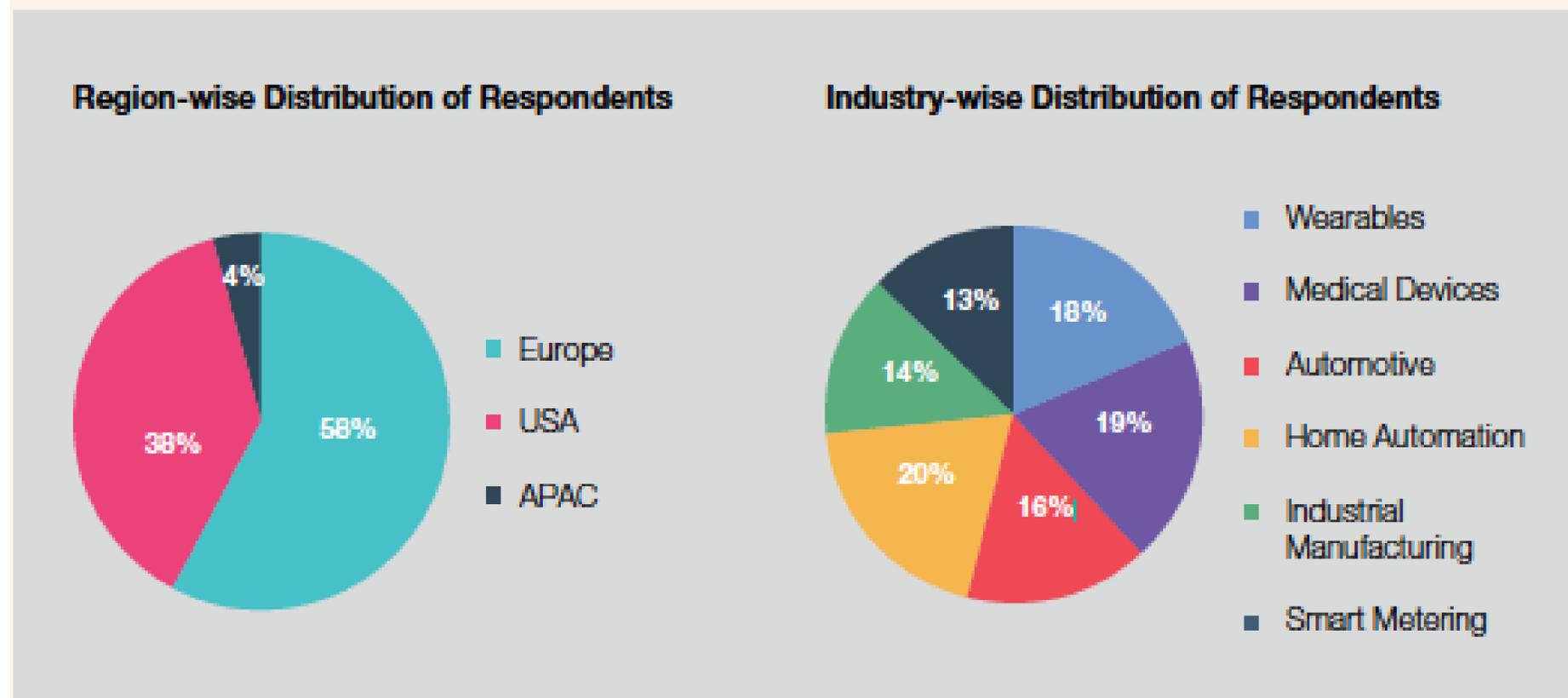
- L'Internet degli Oggetti è l'estensione di Internet al mondo degli oggetti e dei luoghi. Attraverso chip e sensori gli oggetti possono interagire tra loro e con la realtà circostante. Il mondo fisico, a tendere, può essere digitalizzato, monitorato e virtualizzato.
- Secondo Gartner, l'IoT è uno degli elementi disruptive per molti comparti industriali e Capgemini stima che tra 5 anni il 33% della popolazione mondiale indosserà almeno un Wearable o Fitness Device, il 20% degli autoveicoli sarà dotato di dispositivi connessi mentre nel 38% delle nostre case sarà presente almeno uno tra sensori per la sicurezza, sensori bianchi o robot per la pulizia.



IoT

- L'indagine si è concentrata sulla raccolta di pareri sulle seguenti aree:
gli **attuali livelli di sicurezza** dei prodotti IoT, **le sfide chiave** che le organizzazioni devono affrontare per la sicurezza dei loro prodotti IoT e **sull'approccio per mettere in sicurezza** i devices IoT.
- Inoltre sono state analizzate le **politiche privacy** adottate per i dati raccolti da dispositivi IoT e sono state valutate in base al livello di **trasparenza** fornito agli utenti, alla **modalità di raccolta dei dati, al trattamento e alla condivisione con terzi**.

Survey Demographics



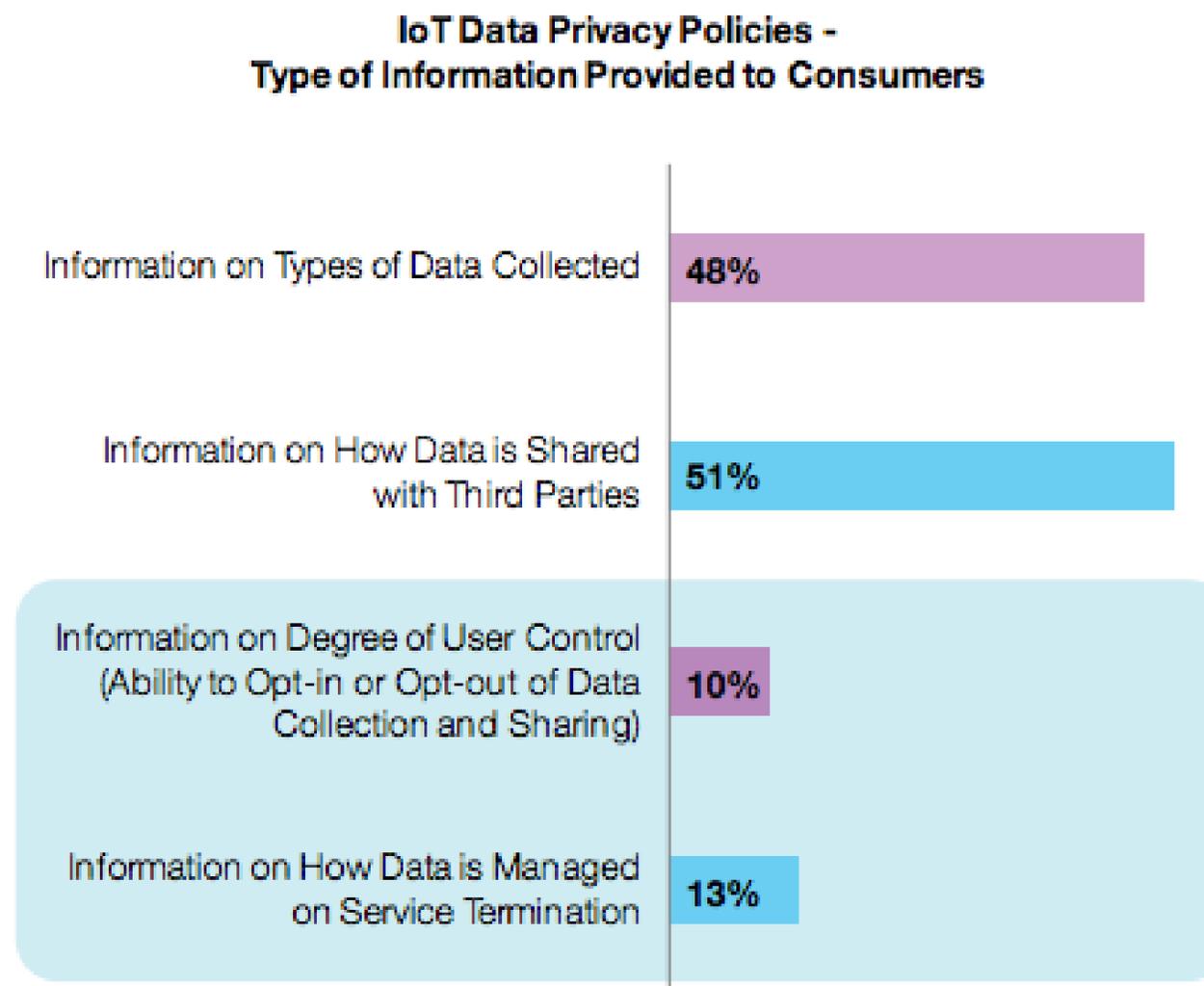
L'indagine ha raggiunto più di 100 dirigenti dei settori coinvolti nello sviluppo dell'IoT, di differenti segmenti di mercato, tra cui Wearables, dispositivi medici, Automotive, Domotica, Smart Metering, e produzione industriale.

<https://www.uk.capgemini.com/resources/securing-the-internet-of-things-opportunity-putting-cybersecurity-at-the-heart-of-the-iot> - Indagine Capgemini Consulting e Sogeti High Tech del 12 febbraio 2016.

IoT

- La sfida più complessa non sembra tanto quella tecnologica o quella dei nuovi modelli di business, ma piuttosto quella della **gestione dei dati** – specialmente quelli sensibili – prodotti dai sistemi connessi sempre più diffusi nelle case, nelle auto, nelle città.
- In un mondo in cui l'IoT è destinato a crescere con lo stesso ritmo degli attacchi informatici rivolti agli oggetti connessi, il tema della **privacy e della data protection** si fa sempre più cruciale.

Figure 4: Data Privacy Information Provided by Organizations



N = 100

Source: Capgemini Consulting and Sogeti High Tech Analysis

Internet delle cose, allarme privacy: dati a rischio negli oggetti smart

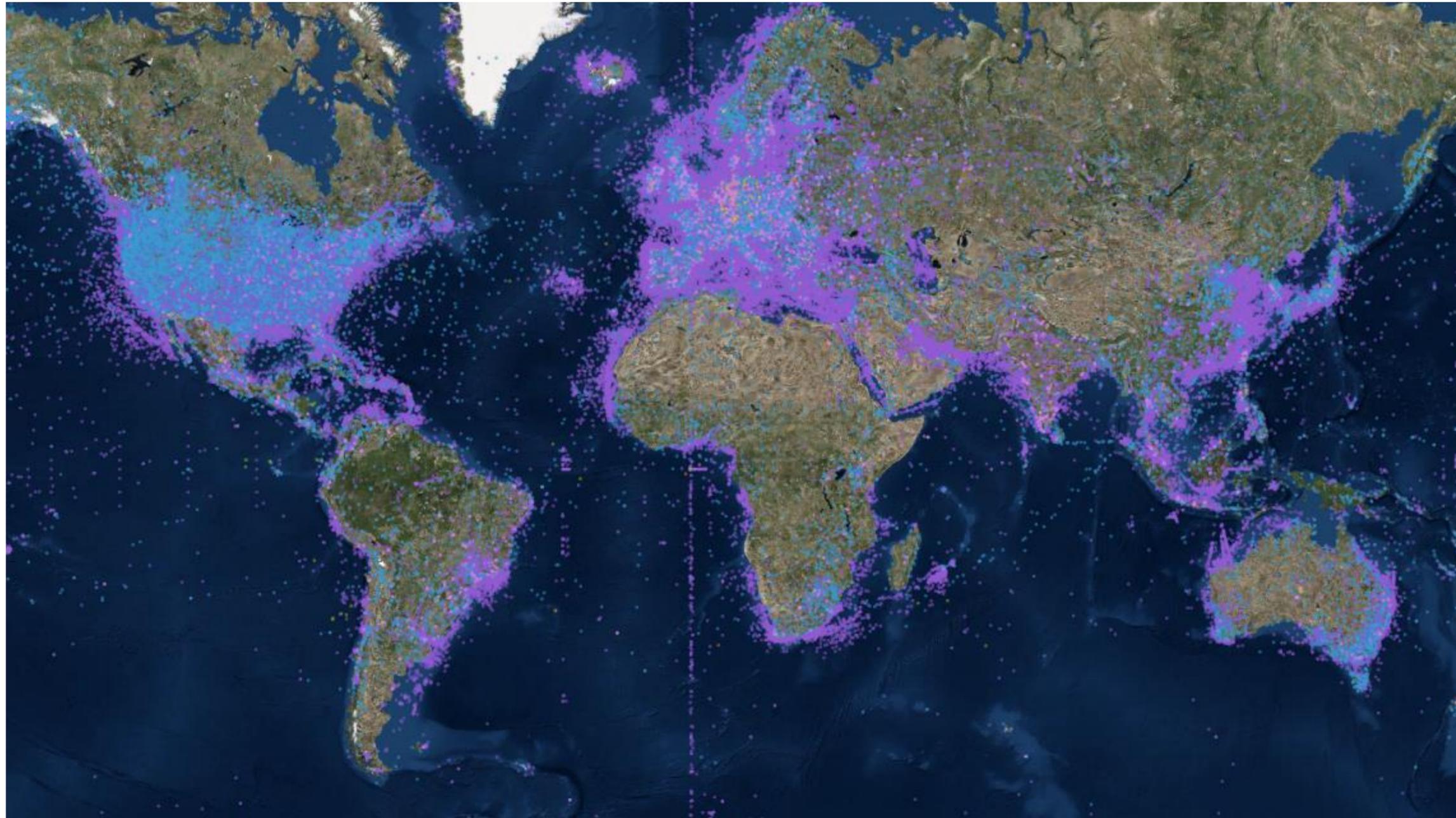
Indagine a tappeto (“sweep”), a carattere internazionale, avviata lo scorso maggio dalle Autorità per la protezione dei dati personali appartenenti al Global Privacy Enforcement Network (Gpen), di cui fa parte anche il Garante italiano, per verificare il rispetto della privacy nell’IoT.

- 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

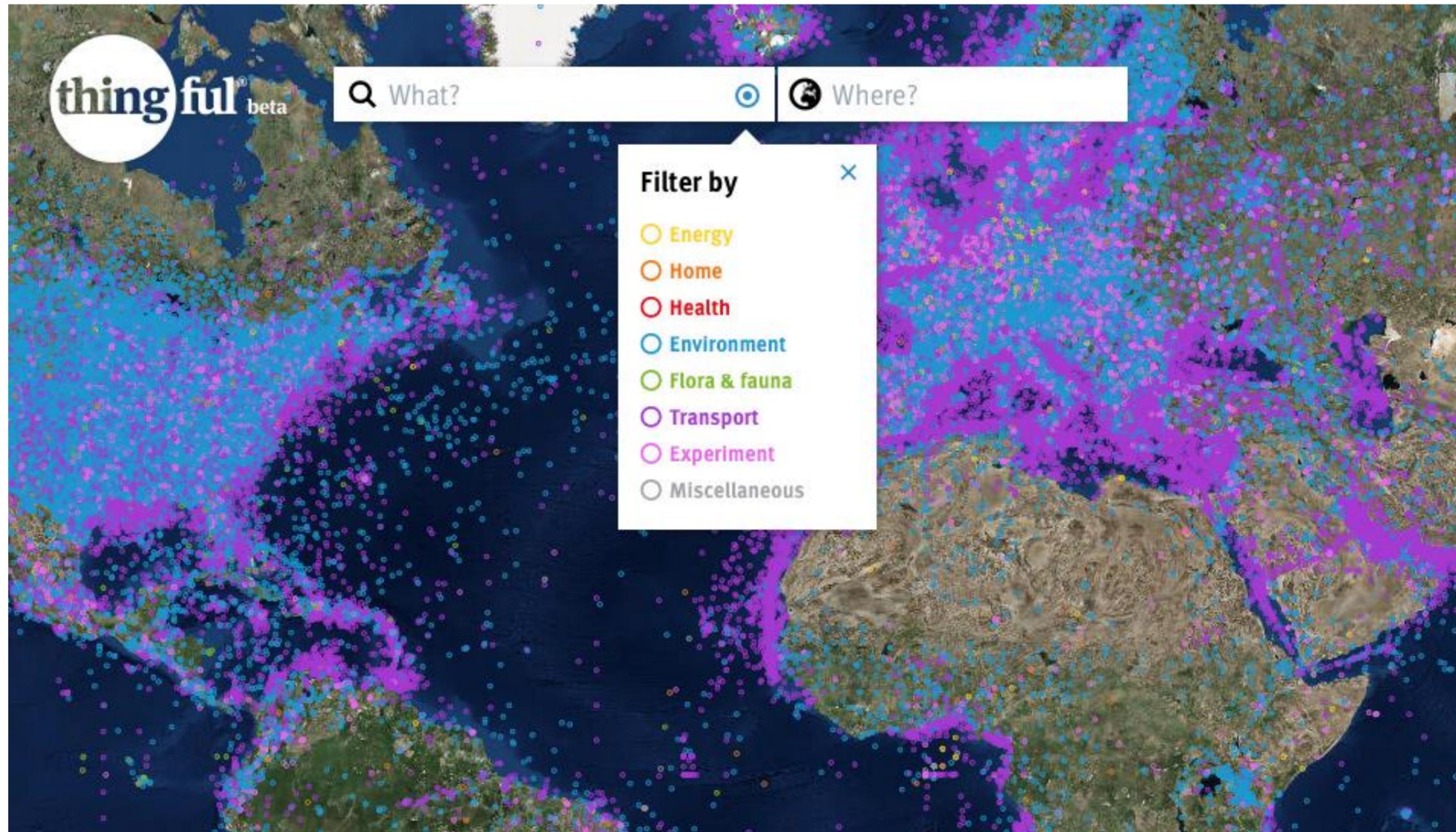


http://www.corrierecomunicazioni.it/digital/43505_internet-delle-cose-allarme-privacy-dati-a-rischio-negli-oggetti-smart.htm

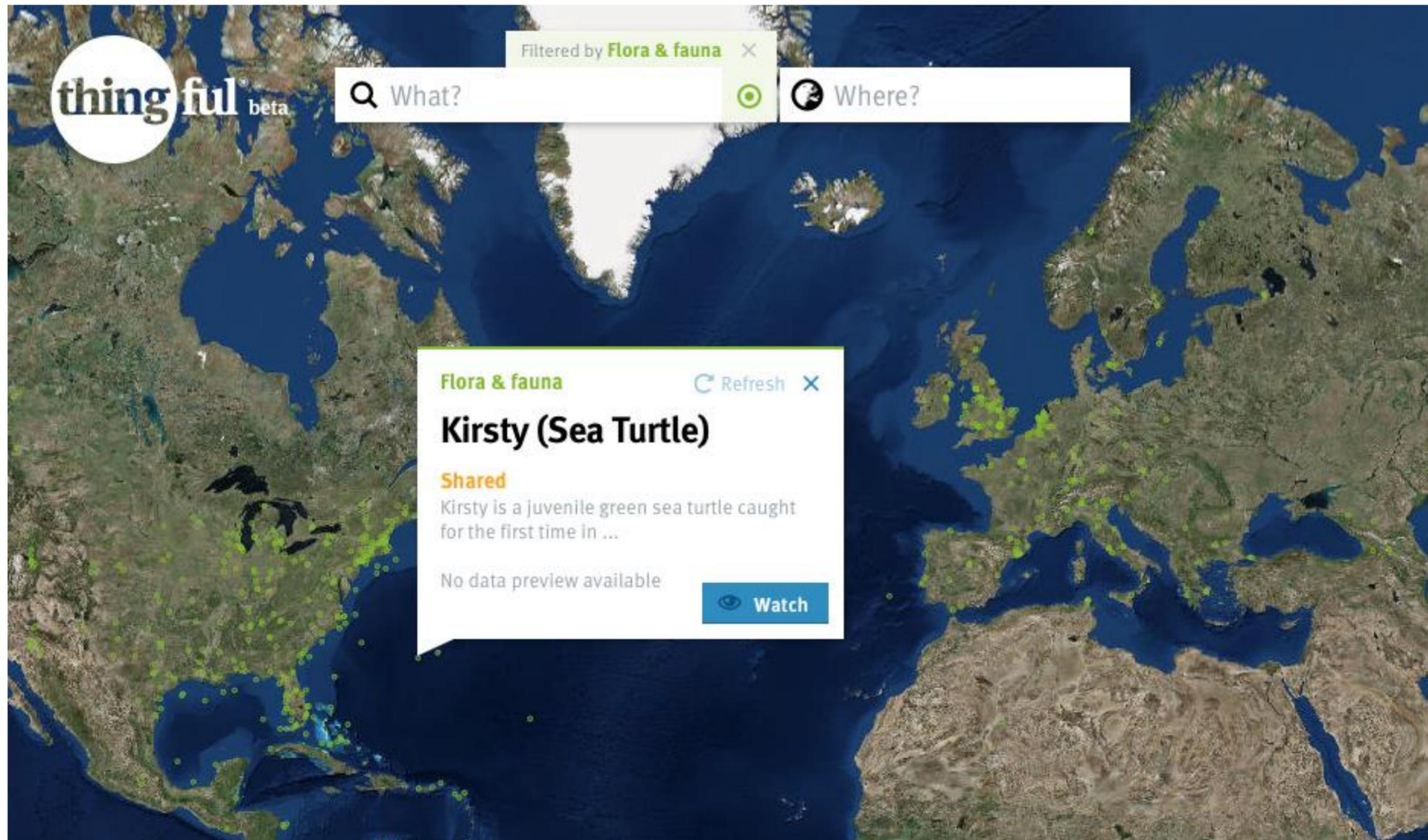
Mappa IoT - <https://thingful.net>



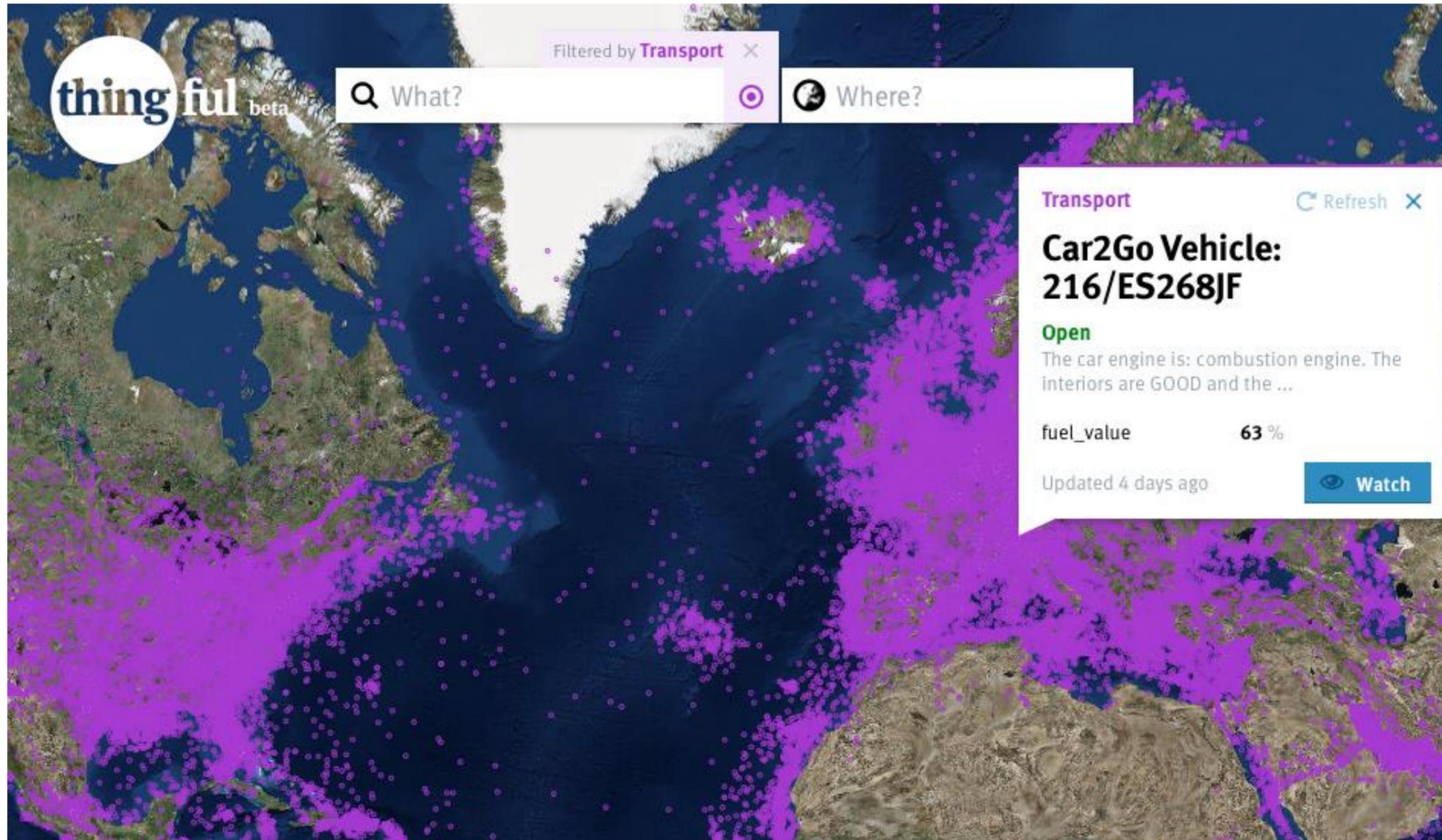
Mappa IoT - <https://thingful.net>



Mappa IoT - <https://thingful.net>



Mappa IoT - <https://thingful.net>



Big Data

- I Big Data sono l'altra grande leva, sempre secondo Gartner, in grado di generare innovazione in molti comparti industriali.
- IoT contribuisce notevolmente ad alimentare i Big Data, spesso producendo volumi di dati esigui ma molto frequenti, ampiamente distribuiti e spesso non strutturati, prodotti ad una velocità vertiginosa.
- Dalla ricerca Cisco del 2015 risulta che per utilizzare in modo efficace le soluzioni IoT, occorre migliorare maggiormente la componente "dati" (per il 40%), i processi (per il 27%), il personale (per il 20%) mentre gli oggetti si attestano in fondo (per il 13%)
- Le aziende devono sfruttare efficacemente l'integrazione, l'automazione e l'analisi dei Big Data per generare informazioni dettagliate e fruibili e massimizzare il valore degli investimenti in IoT.
- Sarà altresì indispensabile colmare la carenza di esperti di sicurezza informatica.
Fino ad ora la sicurezza si è concentrata sulle appliance di Sicurezza e sul perimetro, ma quando si connette ciò che un tempo non era connesso, si formano nuovi varchi.

Digital Transformation

Executive Summary Cisco 2015 -
Come realizzare valore da IoT:
come passare dalla connessione
degli oggetti all'acquisizione di
informazioni pertinenti.

An aerial photograph of a wind farm with several white wind turbines on a green field. A semi-transparent white box with rounded corners is overlaid on the image, containing the text 'Sintesi' and a numbered list of three points.

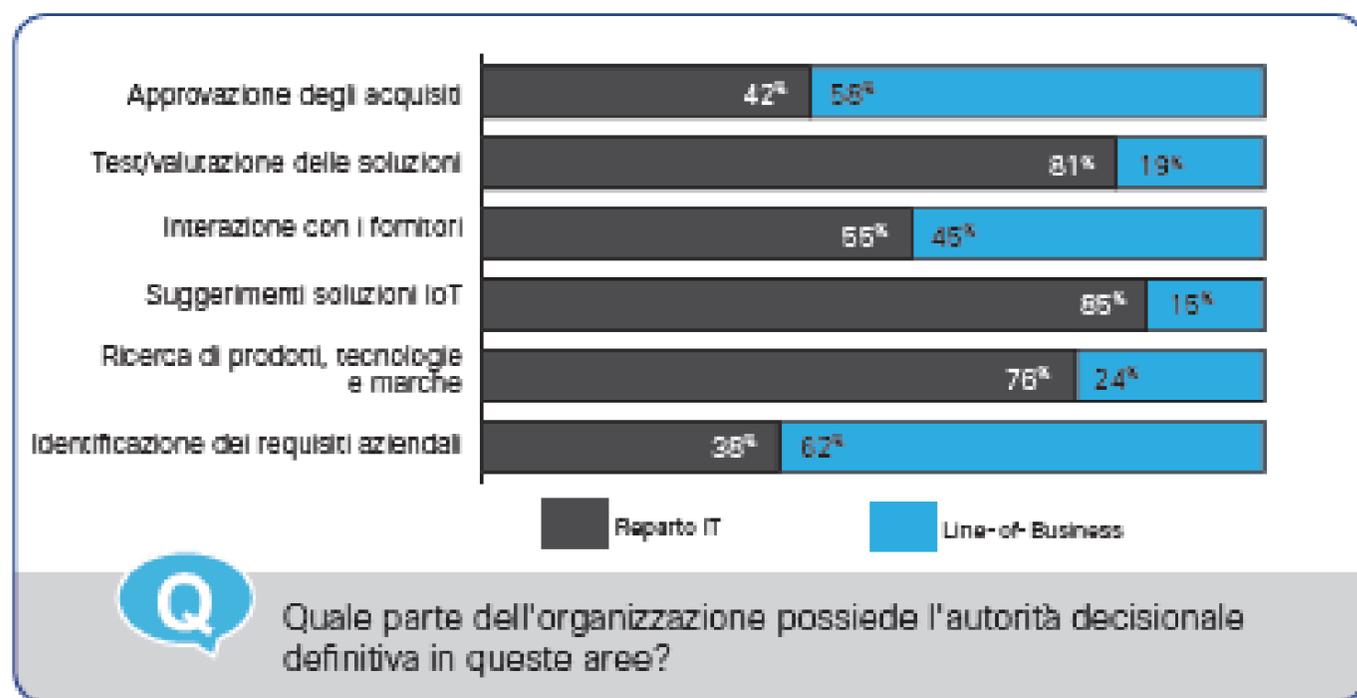
Sintesi

1. Internet of Things (IoT) offre alle aziende del settore pubblico e privato un'opportunità senza precedenti di creare nuove fonti di valore, come la possibilità di automatizzare fino al 50% i processi manuali.
2. Tale valore sarà accessibile alle aziende che puntano a migliorare le proprie capacità dati, quali integrazione, automazione e analisi, e l'agilità dei processi in generale, non a quelle aziende che si limitano ad aumentare il numero dei dispositivi connessi alla rete.
3. Per centrare l'obiettivo, serve una forza lavoro dotata di competenze nuove, una collaborazione efficace fra IT e OT, un vasto ecosistema di partner e un approccio a piattaforma.

Digital Transformation

- I Responsabili OT/Lob avranno autorità decisionali all’inizio e alla fine del processo di adozione, ossia durante l’identificazione dei requisiti aziendali e l’approvazione degli acquisti.

Figura 7
In futuro i dirigenti IT e OT
condivideranno responsabilità superiori per le soluzioni IoT.



Fonte: Cisco Consulting Services, 2014

- Al contrario, il reparto IT dovrà guidare le decisioni relative alle fasi specifiche dell’implementazione, come la ricerca di soluzioni, l’interazione con i fornitori, nonché suggerimenti e testing sulle soluzioni da adottare.
- Per progredire in campo IoT, le aziende dovranno promuovere la **massima** collaborazione fra i responsabili **IT e OT**, in modo da assicurare convergenza verso i risultati di business desiderati.

II GDPR

- **Il GDPR non fa distinzione sulla provenienza dei dati da proteggere**
 1. I consumatori devono avere **fiducia** nel modo in cui vengono utilizzati i loro dati: informativa trattamenti - controller e processor - tempo
 2. I consumatori devono avere il **governo** dei propri dati: controllo - diritto all'oblio – portabilità dei dati
 3. I **dati non sono tutti uguali**: anonimizzazione
 4. La tecnologia è parte significativa della soluzione? Sì, ma non basta.

II GDPR

- Gli obiettivi del GDPR comprendono le indicazioni per migliorare la sicurezza e la data protection dell'IoT e dei dati generati, direttamente o indirettamente, **intervenendo sia sul Titolare che sui soggetti interessati**.
- Le operazioni di scambio ed elaborazione di informazioni sottese dal mondo IoT configura a tutti gli effetti un **trattamento**, sebbene non sempre percepito come tale.
- Tale difetto di awareness da parte dell'utente è in parte imputabile alle nuove modalità di interazione automatica su cui si basa IoT e in parte alla inadeguatezza delle informative fornite
- Il regolamento si applica anche ai dati che identificano un individuo **indirettamente**, come alias, pseudonimi e indirizzi IP. Il che significa che il GDPR ha una portata molto più ampia.
- Il consenso dovrà essere ottenuto dagli interessati se i loro dati devono essere utilizzati per la **profilazione**

II GDPR

- I **nuovi profili di rischio** emersi dalle tecnologie basate sul dialogo tra devices determina l'esigenza di fornire **un'informativa idonea** con particolare attenzione alle finalità del trattamento
- Il WP29 precisa che affinché il trattamento possa considerarsi lecito, "users must remain in complete control of their personal data throughout the product lifecycle" (c.d. principle of self-determination of data)
- La nozione di **controllo** sui dati viene a coincidere con la consapevolezza effettiva circa la destinazione degli stessi, nonché circa le potenziali **utilizzazioni ulteriori** rispetto alla erogazione del servizio richiesto dall'utente.
- In particolare l'Opinion citata pone l'accento sui rischi connessi all'uso successivo delle informazioni raccolte, anche attraverso l'incrocio dei dati inizialmente trattati, per finalità diverse, attraverso i sistemi di analisi (c.d. **crossing-matching**).
- Il trattamento dei dati deve essere sorretto dal **consenso in ogni sua fase**; l'eventuale riutilizzo dei dati per finalità ulteriori, necessita di una nuova manifestazione di consenso da parte dell'interessato.
- *Opinion 8/2014 on the on Recent Developments on the Internet of Things - Adopted on 16 September 2014 (This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy)*

II GDPR

- A ciò si aggiungono le criticità legate alla elaborazione dei dati da parte di soggetti terzi – diversi dal titolare – i quali possono impiegare le informazioni acquisite per scopi ignoti all’interessato: il rischio è l’estromissione del data subject dall’esercizio del reale controllo sui propri dati
- Al riguardo il GDPR pone l’accento sulla necessità di adottare un nuovo approccio concettuale secondo cui la **data protection** non sia uno strumento rimediale e successivo rispetto al trattamento dei dati, bensì una **componente intrinseca dell’architettura del dispositivo** o dell’applicazione (privacy by design)
- E’ il caso delle “stiky policies”, che si basano sull’incorporazione dei **limiti e dei termini** di utilizzo dei dati all’interno dei dati stessi, nell’ottica di un effettivo controllo esercitato dallo user. Ovvero, il consenso al trattamento circola insieme ai dati stessi, definendo le condizioni di utilizzo per le richieste di accesso ai dati da parte di terzi.

II GDPR

- Stessa logica di anticipazione della tutela della riservatezza al momento della progettazione è alla base del **PIA (Privacy Impact Assessment)**, anch'esso presente nel GDPR, per una valutazione prognostica dell'impatto dei dispositivi IoT sui potenziali profili di rischio, prima della immissione sul mercato e in occasione di modifiche.
- Analoga conseguenza deriva dall'introduzione da parte del GDPR del concetto di **portabilità dei dati** (ovvero la possibilità di spostare i dati tra diversi applicativi, ambienti e servizi cloud) estendendo il diritto vigente degli interessati di *accesso*, all'obbligo ai Titolari di fornire i dati in un formato leggibile da un altro Titolare (riduzione rischio locked-in).
- In conclusione, il GDPR pone l'accento sulla presa di coscienza che gli attuali meccanismi di tutela della riservatezza, incentrati su interventi reattivi, sono obsoleti e inadeguati.

Esperienza Portale MY HOME Bticino

MyHOME_Web

bticino

Sei un installatore?

[ENTRA NELL'AREA PROFESSIONISTI](#)

Benvenuto nel portale My Home Web



Con My Home Web
entri in casa tua in modo sicuro ovunque ti trovi

Form di autenticazione

Login

Password

ACCEDI

Hai dimenticato la password? [Clicca qui.](#)
Hai un codice di attivazione? [Clicca qui.](#)

Scopri My Home Web

- Scopri My Home WEB
- Documentazione
- Conosci la domotica

Call Center

Hai dubbi o problemi
sul portale? Chiama il
nostro numero verde.

Numero Verde
800-837035

*(Il numero è attivo dal lunedì al venerdì dalle 8.30
alle 18.30)*



Grazie

@ aused@aised.org

+39 345 255 9509

@aisednews

AUSED

Aused Review