Lawful Interception Academy (LIA)

Atti dell'edizione 2015 della LIA svoltasi a Roma, lido di Ostia, dal 2 al 6 novembre 2015 presso la Scuola di Polizia Tributaria della Guardia di Finanza. La Lawful Interception Academy, è un corso normativo-tecnico di alta formazione sugli strumenti utilizzati per le indagini e per la ricerca della prova relativamente alle vecchie e nuove tecnologie di comunicazione. La LIA è stata fondata nel 2014 da "Sicurezza e Giustizia" e rappresenta il passaggio in "aula" dell'attività didattica svolta dalla rivista su "carta". La LIA è destinata esclusivamente ad appartenenti della PA ed è per questi gratuita, seguendo la stessa impostazione della rivista. La LIA si avvale dei più moderni sistemi di mobile learning.

di Donatella Proto

INTERNET OF THINGS E M2M. IL MERCATO DEL FUTURO E LE PROBLEMATICHE DI SICUREZZA

***Donatella PROTO** è Dirigente della Divisione 2 del MISE "Reti e Servizi di comunicazione elettronica ad uso pubblico della Direzione Generale per i servizi di comunicazione elettronica, di radiodiffusione e postali". Componente dell'Osservatorio per la sicurezza delle reti e delle comunicazioni di cui al decreto del 14 gennaio 2003, come modificato dal decreto dell'5 settembre 2010.*

1. Introduzione

La crescente urbanizzazione a livello globale (si consideri che oggi il 54% della popolazione mondiale e il 73 % della popolazione UE vive in città ed entro il 2050 tali percentuali raggiungeranno rispettivamente il 66% e l'80%) impone di considerare le città come laboratori dove sperimentare misure in grado di generare crescita economica e sviluppo sociale, assicurando nel contempo un ambiente sicuro ed una comunità resiliente.

Non a caso l'Organizzazione delle Nazioni Unite sta attuando, nell'ambito del *Millennium Development Goal n. 11*, il progetto *United Smart Cities*, affinché tutte le città del mondo diventino sostenibili, inclusive, resilienti ai disastri e sicure. La Smart City è un modello urbano economicamente e socialmente sostenibile che garantisce un'elevata qualità della vita dei cittadini, una crescita della competitività delle imprese ed un rafforzamento della capacità istituzionale e di investimento delle amministrazioni in un ambiente sicuro. Tale modello si basa sulla diffusione da un lato di piattaforme tecnologiche e di connettività in grado di abilitare la creazione di ecosistemi di servizi digitali grazie ad infrastrutture ICT e TLC e dall'altro della cd IoT (Internet of Things).

La "*Internet of Things*" è un sistema complesso e che richiede un'ampia *governance* normativa, regolamentare, tecnologica e di mercato. In tale sistema, sensori incorporati negli oggetti fisici più disparati vengono collegati tramite reti wired e wireless, utilizzando lo stesso protocollo che si connette ad Internet. L'enorme quantità di dati generata dai sensori viene utilizzata per specifiche analisi, dalle quali possono derivare nuovi modelli di business e di governance finora inesplorati: da una consultazione svolta dalla Commissione Europea nel 2013 è emerso chiaramente che la IoT è fra le soluzioni con il più elevato potenziale per migliorare la vita dei cittadini UE.

L'irreversibilità dell'evoluzione tecnologica, la possibilità di sviluppo delle imprese e la mole di nuovi servizi disponibile per i cittadini e per le amministrazioni sottese dalla IoT rappresenta un valore rispetto al quale è necessario porsi, però, con il dovuto livello di attenzione, soprattutto perché un'evoluzione destrutturata del mercato, senza una guida adeguata da parte dei Policy makers, potrebbe comportare rischi di vario genere, come tratteremo meglio nel seguito.

Tra i servizi appartenenti alla tipologia della "*Internet of Things*", un approfondimento specifico meritano i servizi denominati Machine to Machine (M2M), in quanto caratterizzati da alcune peculiarità quali lo scambio automatico dei dati tra i dispositivi e/o applicazioni IP based (quasi sempre) e nessuno o ridotto intervento umano.

Il contesto nel quale i servizi M2M si stanno sviluppando è, però, attualmente di decisa deregolamentazione e se questa può essere un'opportunità da alcuni punti di vista, per i medesimi motivi può essere un rischio, in particolare per aspetti legati a temi quali:
1) la tutela della privacy (o *rectius* dell'identità personale) con facile accesso ad informazioni che diventano sempre più strategiche per modelli di business real time, con la conseguente necessità di definire anche nuove forme di responsabilità,
2) la sicurezza non solo delle comunicazioni, in modo da evitare danneggiamenti, manipolazioni o distruzioni anche all'insaputa

del titolare del dato, dei prodotti o dei dispositivi, tale per cui è necessario garantire la sicurezza delle persone attraverso una concreta applicazione dei paradigmi e delle strategie basate sul cd. approccio di *privacy and data protection by design (implementando, cioè, i requisiti di sicurezza sin dalla fase di progettazione del dispositivo) ed* evitando, però, tecniche di cifratura e di anonimizzazione dei dati che hanno l'obiettivo di rendere i dati non più identificabili sottraendoli in questo modo alla applicabilità della normativa privacy, ma anche e non da ultimo la sicurezza nazionale, con la necessità di ripensare (forse) la strategia nazionale sulla cybersecurity, rifuggendo, però, da qualsiasi atteggiamento tecnofobo.

2. Smart City ed Urban Security

Una delle principali situazioni in cui le tecnologie dell'Internet of Things avranno, nel breve periodo, una particolare rilevanza sono - come anticipato - le *Smart Cities*, ove si impone la necessità di *policy* che assicurino elevati standard di sicurezza delle reti, dei sistemi informatici, dei dispositivi, delle applicazioni che sono alla base degli ecosistemi di servizi digitali su cui esse si basano. Il cambiamento delle città in senso *Smart* richiede, infatti, che le informazioni sulle quali si basano i servizi, già di per sé a volte molto sensibili, siano raccolte e trattate con riservatezza ed integrità.

Gli standard di sicurezza che devono connotare servizi e dispositivi diffusi all'interno dell'Internet of Things devono essere tali da contrastare l'evenienza che essi siano interrotti, corrotti o addirittura deviati, causando gravissimi danni alle persone, alla tutela della vita privata e delle attività economiche, ed in definitiva all'immagine stessa di tutte le iniziative volte a realizzare delle Smart Cities.

Il fattore abilitatore del modello Smart Cities sono le tecnologie ICT, in quanto capaci di "teleacquisire" grandi quantitativi di dati, elaborarli in tempi brevi e creare quella piattaforma informativa, aperta e condivisa, indispensabile per i decisori istituzionali, ma affinché questa mole di dati possa essere processata intelligentemente e si possano evitare pericolose deviazioni il contesto in cui si opera deve essere per l'appunto assolutamente sicuro, considerando le sue articolazioni e la marcata interdipendenza settoriale, tra attori pubblici e privati, tra amministrazioni centrali e locali, tra interessi che possono essere o apparire confliggenti. Risulta, pertanto, indispensabile un forte controllo del percorso di avvicinamento di tutti i soggetti pubblici, ed a cascata di quelli privati da coinvolgere nella fase attuativa, al rispetto di stringenti paradigmi tecnici ed amministrativi per l'attuazione di un sicuro e sostenibile modello di "smart cities".

Altro punto cardine per lo sviluppo di un sicuro e sostenibile modello di "smart cities" è un confronto permanente con la società civile nella fase di acquisizione dei bisogni, ma anche nella fase di traduzione degli stessi in requisiti e nella fase di monitoraggio dell'efficacia degli interventi previsti per il loro soddisfacimento. Bisognerebbe iniziare a considerare *la civic partecipation* come forma di prevenzione dei problemi, fonte di conoscenza e strumento d'azione, partendo da una nuova idea di cittadinanza, per cui la disponibilità di informazioni e conoscenza possa sviluppare nel singolo soggetto maggiore consapevolezza ed un ruolo maggiormente attivo sul piano sociale in una visione utente-centrica, che presuppone, però, il superamento di un divario digitale non solo infrastrutturale ma anche e soprattutto socio-culturale.

Ma per il raggiungimento di tale obiettivo una delle principali criticità, da risolvere *ex ante*, è evidentemente quella del miglioramento, dell'omogeneizzazione della conoscenza e della possibilità di insediare, all'interno delle strutture organizzative dei soggetti pubblici coinvolti, nuclei stabili di competenze che integrando informazioni generino "intelligenza".

Una città intelligente è anche una città sicura, ove per sicurezza deve intendersi non solo la sicurezza personale, ma anche la sicurezza sociale, la sicurezza delle infrastrutture fisiche ed informatiche, la sicurezza stradale, la sicurezza del patrimonio naturale e culturale.

Se è di più immediata percezione ed evidenza quanto le tecnologie avanzate possano coadiuvare nella prevenzione e nella repressione dei fenomeni di illegalità e delle situazioni che creano allarme sociale, considerando che negli ultimi anni sono in aumento i reati contro il patrimonio e conseguentemente il senso di insicurezza della popolazione, soprattutto di certe fasce di età e di sesso (come donne ed anziani), allora è bene soffermarsi anche sull'ausilio che le tecnologie possono dare sia in tema di riduzione dei danni alle infrastrutture (e quindi ad esempio in tema di sicurezza stradale), sia in tema di riduzione dei danni all'ambiente, sia che essi siano riconducibili ad eventi climatici sia che siano riconducibili all'azione dell'uomo.

3. Smart and Green Mobility: verso una mobilità partecipata e sicura

L'applicazione delle tecnologie informatiche e della comunicazione ai sistemi di trasporto, alle infrastrutture viarie (e non solo), ai veicoli ed alla gestione del traffico e della mobilità è diventato una dei **settori di intervento strategico non solo** per le telco (e OTT), per *car makers* e produttori dell'indotto**, ma per il sistema Paese**, in quanto porta non solo un aumento della produttività e della competitività nel comparto, migliori servizi per i cittadini, sia in termini di costo che di qualità, accessibilità a servizi avanzati, anche per soggetti in *digital divide*, ma soprattutto **maggiore sicurezza sulla strade,** ponendosi come obiettivo la prevenzione degli incidenti (il 95% dovuto ad errori umani), il miglioramento del traffico, la riduzione dei consumi e, quindi, dell'impatto ambientale, sia in termini di quantità di emissioni di CO_2, che di rumore.

Se da un lato, infatti, la filiera Automotive costituisce uno dei pilastri industriali e di sviluppo del sistema Paese, come dimostrano i dati di seguito riportati (*Fonte Ania 2014)*:

- **3.200** le imprese automotive
- **275.000** gli addetti nella filiera produttiva pari all'**7%** degli occupati nel settore manifatturiero
- **88** miliardi di euro di fatturato pari al **5,5** %del Pil
- **3** miliardi di euro spesi in R&D
- **37.080.753** le autovetture circolanti, di cui **1.360.501** di nuova immatricolazione
- **39** miliardi il valore del mercato globale delle *Connected Cars* nel 2018, partendo dai € **13** miliardi del 2012
- **22%** delle automobili vendute su scala globale hanno a bordo soluzioni di connettività wireless: una percentuale che si stima raggiungerà l'**89**% nel 2024.
- **2** milioni le "Scatole Nere" circolanti in Italia, pari al 6% del parco assicurato totale, con una previsione di crescita al 2017 fino al 10-15% (pari a circa 5,7Mln di Scatole Nere)

dall'altro esistono tali e tanti problemi in termini di Sicurezza, Congestione delle strade ed Ambiente, che impongono come non più differibile un approccio integrato per sviluppare una mobilità sostenibile.
Tra le applicazioni per la sicurezza un ruolo prioritario rivestono non solo i sistemi di tracciamento delle merci (si pensi a merci di pregio o pericolose) e dei veicoli, ma anche i sistemi di ausilio alla guida e gestione delle emergenze come l'eCall (tra i servizi M2M non IP based), per cui l'EU ha imposto una scadenza:

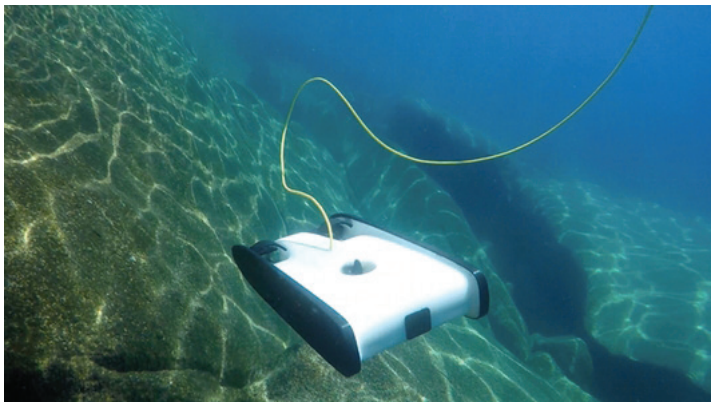
"L'eCall sarà obbligatorio dal marzo 2018 per tutte le auto di nuova immatricolazione"
"L'eCall è l'esempio perfetto di un progetto sviluppato dalla Ue per salvare vite umane. Adesso la legge permetterà di fornire vantaggi reali grazie alle tecnologie digitali", ha detto **Günther H. Oettinger**, commissario Ue all'Economia Digitale.

In caso di grave incidente una chiamata eCall viene avviata automaticamente (o manualmente) dal dispositivo veicolare, creando una connessione vocale che invia automaticamente un messaggio dati (MSD) relativo all'incidente. La chiamata, identificata come eCall dalla rete mobile, viene istradata al PSAP (Public Safety Answering Point) che decodifica l'MSD ricevuto ed avvia la gestione dell'incidente, inoltrando i dati ad una sala operativa o ad un altro PSAP.
L'MSD include: a) l'orario dell'incidente; b) la localizzazione del veicolo; e c) la direzione di marcia

Da un veicolo meramente connesso ci si proietta verso un veicolo cooperativo, in cui l'automobile diventa sensore e fonte di informazioni di traffico e di sicurezza, operante su una piattaforma telematica «aperta ed integrata», in cui il dispositivo di bordo, che implementa l'eCall, può essere usato per abilitare anche altri servizi a valore aggiunto nello spirito della direttiva UE ITS (Direttiva 2014/40/CE del 6.7.2010) con l'obiettivo di avere un Paese più veloce, più informato, più sicuro, più *smart*. I dati così raccolti alimentano centri di controllo e supervisione che attraverso *enabling platforms* possono gestire in misura coordinata le esigenze di sicurezza in mobilità, quelle della sicurezza urbana e del territorio. Sotto tale profilo il tema delle Smart Cities si intreccia con la realizzazione delle cd reti PPDR (***Public Protection and Disaster Relief***): si tratta di reti radio a banda larga progettate per poter rispondere all'esigenza di un'infrastruttura radio efficiente, in grado di supportare le operazioni di soccorso su vasta scala, che possano derivare da eventi emergenziali di qualunque tipo, derivanti sia da motivi naturali (p.e. vaste inondazioni, incendi, frane etc) che umani. Le operazioni di protezione civile e/o di pubblico soccorso utilizzano in modo pesante l'accesso ai dati distribuiti sui database delle organizzazioni coinvolte nella gestione delle emergenze - come la polizia, i vigili del fuoco, la protezione civile (nelle sue declinazioni centrali e regionali) e l'emergenza sanitaria. Le reti PPDR devono essere in grado di gestire volumi elevati di scambio dati in modo sicuro: queste informazioni comprendono immagini, mappe e progetti architettonici degli edifici. Allo stesso modo il flusso di informazioni di ritorno da unità in campo per i centri di controllo operativi dovrà essere trattato con analoga priorità: durante una situazione di emergenza, le Autorità responsabili del soccorso sono tenute a prendere decisioni che sono indubbiamente influenzate dalla qualità e dalla tempestività delle informazioni ricevute.

In una visione utente-centrica i cittadini o i *city user* in generale diventano essi stessi fonte di dati e di informazioni e potranno (dovranno) essere coinvolti dalle pubbliche amministrazioni nella valutazione delle politiche di mobilità sostenibile o nella sperimentazione di modalità di trasporto eco-sostenibile o alternativo basata sul modello *"pay per use"*.

4. Ambiente sicuro: l'esempio dello Smart Water Management e l'Internet underwater Things



In tema di sicurezza ambientale il futuro della IoT è anche sottoacqua. Le acque, infatti, sono oramai immense autostrade digitali sulle quali, oltre ai veicoli guidati dall'uomo, operano sensori sofisticati e si muovono robot intelligenti in grado di svolgere compiti pericolosi o che risultano troppo estremi per l'uomo, dal monitoraggio ambientale dei vulcani sottomarini, per la ricerca di idrocarburi o la tutela delle aree marine protette, allo sminamento, alla localizzazione delle persone disperse, fino al controllo dei flussi migratori o alla sorveglianza delle infrastrutture fisiche sensibili: nello svolgimento di tali compiti le tecnologie di comunicazione rivestono un ruolo fondamentale in quanto riescono a riferire da remoto quello che accade sulla o sott'acqua.

L'*Internet underwater Things* è, però, una sfida tutta da vincere in quanto si va ad operare in un mondo ancora largamente sconosciuto. Il dubbio (che appare quasi una certezza alla luce dei progetti europei già avviati su tali temi) è che le tradizionali soluzioni wireless non siano in grado di funzionare o di supportare comunicazioni a lunga distanza, essendo l'ambiente di propagazione l'acqua e non l'aria. La soluzione sta nell'imitare la natura e cioè utilizzare sistemi ibridi di comunicazione (ottici ed acustici) che potranno garantire prestazioni con valori di megabit/sec sia sott'acqua che verso la superficie.

Comunque già oggi la sicurezza dell'ambiente può passare attraverso reti di sensori che consentono di prevenire e gestire i rischi geoidrogeologici e di erosione costiera, i fenomeni alluvionali e delle frane in scenari di repentino cambiamento climatico, anche attraverso meccanismi di allerta precoce, come in caso di acqua alta nella città di Venezia.

5. Alcune riflessioni finali: la IoT rappresenta una nuova frontiera per il cybercrime?

Giorno dopo giorno è, quindi, sempre più evidente che quella che sembrava solo fantasia è una realtà da non sottovalutare: se è di sentore comune che le macchine possono diventare uno strumento pericoloso e lesivo per la salute e l'incolumità fisica delle persone, è altrettanto evidente che stante la crescita esponenziale dei dispositivi diffusi all'interno dell'Internet of Things gli standard di sicurezza da implementare debbano essere tali da contrastare l'evenienza che tali dispositivi possano essere interrotti, corrotti o addirittura deviati, sottraendo ad es. informazioni strategiche o sensibili oppure innescando meccanismi di arresto dei servizi e dei sistemi - in alcuni casi anche critici - tali da provocare danni di natura non solo economica, ma anche e soprattutto reputazionali.

Il divario tra realtà e finzione può diventare del tutto inesistente se si pensa alle possibilità odierna di provocare direttamente o indirettamente la morte di un bersaglio scelto attraverso l'intrusione e la violazione della tecnologia.

È recente ad esempio la notizia di come una coppia di hacker in America abbia preso il controllo da remoto di una Jeep che viaggiava in autostrada, sfruttando la vulnerabilità del sistema di connessione wireless installato a bordo. Potendo accedere al sistema centrale diventa possibile modificare la temperatura dell'abitacolo, ma anche governare l'acceleratore, il freno, il cambio e tutta l'elettronica di bordo e, quindi, causare un incidente, anche per il solo fatto che la maggior parte dei guidatori di fronte ad un tale episodio cadrebbe in preda al panico. Ma si pensi anche agli effetti sulla sicurezza stradale se addirittura si innescassero effetti emulativi o a catena.

E se si pensa che il controllo da remoto potrebbe riguardare gli impianti di domotica, i dispositivi biomedici, i dispositivi wearable (l'elettronica indossabile) o un SAPR (Sistemi Aeromobili a Pilotaggio Remoto), affinché i rischi legati alla IoT non diventino tali da vanificare i benefici è indispensabile un'adeguata *governance* ed una altissima attenzione agli aspetti di sicurezza per dissuadere azioni non autorizzate.

A livello globale si sono verificati nel 2013 circa 1.150 attacchi informatici, di cui 35 in Italia con danni annuali tra i 2 e i 4 miliardi di euro nel solo Belpaese e circa 110 miliardi a livello globale

"*Il crimine informatico* – si sottolinea nella Strategia nazionale sulla cybersecurity - *è una piaga che può decretare il fallimento delle aziende, la sottrazione del loro patrimonio tecnologico e che depaupera la ricchezza delle Nazioni. Con sempre maggiore preoccupazione assistiamo, inoltre, al crescere di una minaccia ancora più insidiosa, che sfrutta la vulnerabilità dei sistemi informatici per sottrarre il frutto del nostro lavoro di ricerca e sviluppo nel campo delle nuove tecnologie e dei prodotti. Per un Paese come l'Italia, che fa dell'innovazione la pietra angolare della sua crescita e della sua competitività, il danno potenziale è incalcolabile*".

Certamente non si può fermare il cambiamento, ma bisogna imparare (in fretta) a gestire la sua complessità. ©