Robot, Intelligenza Artificiale e le nuove sfide per la Sicurezza

TECH AND LAW CENTER

Chi siamo

Il Tech and Law Center (TLC) è un centro di ricerca multidisciplinare promosso da un gruppo di lavoro composto da membri dell' Università di Milano, Università di Milano–Bicocca, Università dell'Insubria e Politecnico di Milano. Attraverso le attività del centro si vuole promuovere la conoscenza e la comprensione del mondo di Internet e delle nuove tecnologie e della loro interazione con diritto e società.

Giuseppe Vaciago

Giuseppe Vaciago
Partner presso
R&P Legal

Avvocato a Milano e
Professore di Informatica
Giuridica

Giuseppe Vaciago è un avvocato del foro di Milano dal 2002 e negli ultimi 10 anni il suo obiettivo primario è stato il diritto dell'Information Technology con un focus sulla criminalità informatica. Ha assistito molte aziende nazionali e internazionali operanti nel settore IT. E' autore di numerose pubblicazioni in materia di criminalità informatica, sia su riviste che su testi scientifici, che sono stati adottati dalle Università dove insegna. Accademicamente, ha conseguito il dottorato di ricerca sulla Digital Forensics presso l'Università di Milano ed è docente presso l'Università dell'Insubria (Varese e Como), dove tiene un corso di Informatica Giuridica. Ha anche tenuto numerose conferenze e presentazioni in Italia e all'estero.

Ha frequentato la Fordham Law School e la Stanford Law School come Visiting Scholar per espandere i suoi studi nella propria area di ricerca.

E' membro del comitato esecutivo della Tech e Law Center, ricercatore presso il Centro Nexa e presso il Cybercrime Institute di Colonia.

Twitter: @giuseppevaciago

Francesca Bosco

Francesca Bosco

UNICRI
Programme
Officer
Funzionario UNICRI

Francesca Bosco ha conseguito la laurea in giurisprudenza in diritto internazionale e ha iniziato a lavorare nel 2006 presso UNICRI come membro della Unità Crimini Emergenti. All'interno di questa organizzazione è responsabile dei progetti di prevenzione della criminalità informatica e, in collaborazione con partner strategici, ha sviluppato nuove metodologie e strategie per la ricerca e la lotta contro i crimini informatici.

Recentemente, Francesca si sta occupando dello sviluppo di programmi di rafforzamento delle capacità tecniche per contrastare il coinvolgimento del crimine organizzato in criminalità informatica, nonché sull'utilizzo terroristico di internet.

Francesca è uno dei fondatori del Tech e Law Center.

Twitter: @francibosco

Agenda

INTRODUZIONE

POSSIBILI SOLUZIONI

LE SFIDE LEGALI
E DI POLICY

CONCLUSIONI E
RACCOMANDAZIONI

TECH AND LAW
CENTER

Introduzione

Che cos'è l'*Artificial Intelligence* (AI)?

Il termine venne introdotto per la prima volta da John McCarthy nel 1956 (USA).

Non esiste una definizione accettata e condivisa.

In parole semplici: l'AI si prefigge lo scopo di comprendere il funzionamento – in senso olistico della mente umana e riprodurlo in modo, appunto, artificiale.

Considerazioni di contesto sull'*AI*

"La caratteristica più evidente dell'intelligenza artificiale, che la separa dalle tecnologie precedenti, è la sua abilità ad agire autonomamente. Oggi, i sistemi dell'AI sono in grado di svolgere compiti complessi, come guidare una macchina o la costruzione di un portfolio di investimenti, senza il controllo dell'uomo o una supervisione."

Reference: Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies", Matthew U. Scherer, Harvard Journal of Law & Technology, Volume 29, Number 2 Spring 2016

Cos’ è la robotica?

Definizione industriale (RIA - SIRI)

Manipolatore programmabile multiscopo per la movimentazione di materiali, di attrezzi ed altri mezzi di produzione, capace di interagire con l’ambiente nel quale si svolge il ciclo tecnologico di trasformazione relativo all’attività produttiva.

Oggi Intelligenza Artificiale e Robotica sono intimamente connesse ed è proprio questa interazione che pone i problemi giuridici del futuro.

Alcune categorie…

1. *Cyber Physical Systems*

Sistemi ingegnerizzati che integrano gli algoritmi computazionali e i componenti fisici.

2*. Decision Science*

L'utilizzo di algoritmi in grado di sviluppare strategie e decisioni al posto degli essere umani.

3. *Data Products*

L'utilizzo di algoritmi che hanno la capacità di analizzare le informazioni (Big Data) al fine di rendere automatiche le ricerche e le eventuali raccomandazioni.

Considerazioni di contesto su robotica e AI

La prevedibilità e il controllo: i sistemi di AI e robotica possono produrre dei comportamenti imprevedibili. Di conseguenza per gli esseri umani potrebbe essere difficile mantenere il controllo delle macchine programmate per agire con una certa autonomia.

Ubiquità della raccolta dei dati: l'introduzione di sensori, robot e oggetti intelligenti pone nuove sfide e accresce il livello di sensibilità dei dati raccolti.

Il danno potenziale in caso di un uso dei dati non previsto del consumatore: la varietà e il volume dei dati personali e delle informazioni private messe a disposizione di terze parti è enorme e pone rischi per il consumatore e anche le società che devono raccogliere questo tipo di informazioni

Security: ogni tipo di device (*Internet of Things*) o robot connesso a internet è a rischio di essere attaccato. Un livello non adeguato di sicurezza può permettere a terzi di avere accesso a informazioni personali raccolte e trasmesse attraverso tali strumenti.

Danno a persone e cose: IoT e robotica per definizione sono oggetti che, in casi patologici, sono in grado di generare danni a persone e cose.

Esempi pratici – Grandi opportunità

Adnan Farooqui and Eliane Fiolet, Meet Pars, The Aerial Rescue Robot

Esempi pratici – Infiniti Rischi

Todd Humprey: Unmanned Aircraft Capture and Control via GPS Spoofing

Esempi pratici – Infiniti Rischi

To Make a Robot Secure: An Experimental Analysis of Cyber Security Threats Against Teleoperated Surgical Robots

Esempi pratici – Infiniti Rischi

On the Safety of Machine Learning: Cyber-Physical Systems, Decision Sciences, and Data Products

I rischi sono maggiori dei benefici?

I think we should be very careful about artificial intelligence. If I had to guess at what our biggest existential threat is, it's probably that. So we need to be very careful

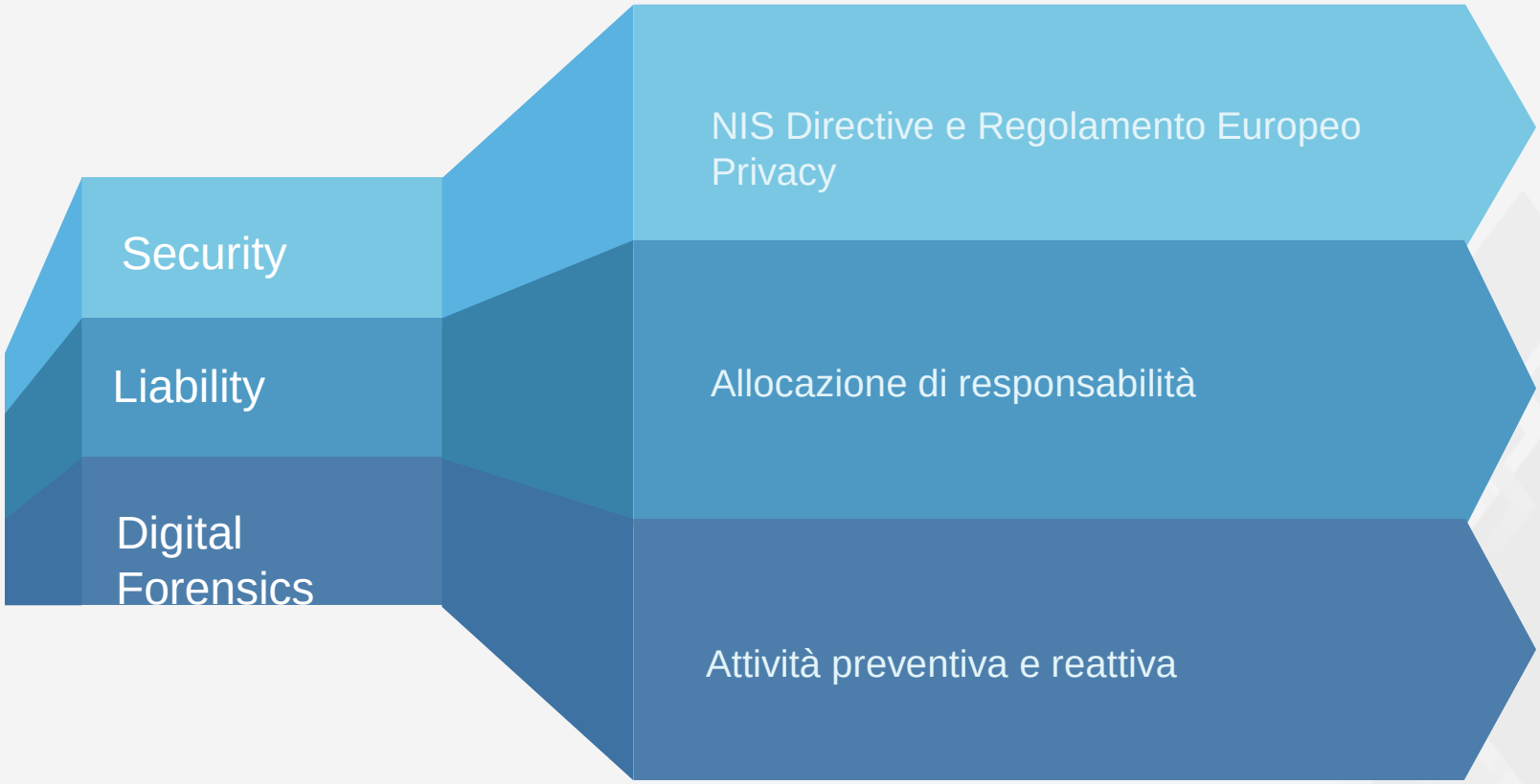
Elon Musk - 2014

Success in creating AI would be the biggest event in human history. Unfortunately, it might also be the last, unless we learn how to avoid the risks.

Stephen Hawking – May 2014

Reference: Independent, Stephen Hawking: 'Transcendence looks at the implications of artificial intelligence - but are we taking AI seriously enough?', May 2014 and The Guardian, "Elon Musk: artificial intellifence is our biggest existential threat," October 2014

Le sfide legali



Security - Il ruolo della NIS Directive

La Direttiva 2016/1149 chiamata anche NIS (**Network and Information Security**) è una normativa che fornisce un livello per i fornitori di servizi essenziali tra cui sono compresi anche i fornitori di servizi digitali. I settori coperti dalla NIS directive sono sostanzialmente quelli legati alle infrastrutture critiche: **energia, trasporti, banche, finanza, salute e settore idrico**. Se è vero che sono ricompresi anche i fornitori di servizi digitali non è ricompreso il settore della robotica e dei suoi produttori. Gli elementi fondanti della direttiva sono:

1. National Information Security Strategy: Obbligo per gli Stati Membri di adottare una strategia nazionale sulla sicurezza delle reti e dei sistemi informativi
2. Rete di Cooperazione: realizzazione di un network europeo che si occupi della sicurezza delle reti critiche.
3. Computer Emergency Response Team (CERT): individuazione per ogni Stato Membro di un'autorità nazionale competente per la sicurezza delle informazioni e creare una squadra di "pronto intervento"
4. Data Breach: vengono stabiliti degli obblighi di notifica in caso di data breach per le società e i fornitori di servizi digitali
5. Point of Contact: vengono imposti degli obblighi per gli Stati Membri di creare dei punti di contatto per lo scambio di informazioni tra le autorità.

Reference: DIGITALEUROPE's, Views on the Internet of Things, Brussels, 14 April 2016

Security - Il ruolo del Regolamento 2016/679

I principali requisiti di sicurezza imposti dal Regolamento Europeo sulla Privacy sono:

1. Un sistema deve poter garantire: (i) la **pseudonimizzazione** e la **cifratura** dei dati personali; (ii) la capacità di assicurare su base permanente la **riservatezza**, l'**integrità**, la **disponibilità** e la **resilienza** dei sistemi e dei servizi di trattamento; (iii) la capacità di **ripristinare** tempestivamente la disponibilità e l'**accesso** dei dati personali in caso di incidente fisico o tecnico; (iv) **Testare**, **verificare** e **valutare** regolarmente l'efficacia delle **misure tecniche e organizzative** al fine di garantire la sicurezza del trattamento (art. 32)

2. Ove possibile, una **descrizione generale delle misure di sicurezza tecniche e organizzative** di cui all'articolo 32 (art. 30)

3. In caso di violazione dei dati personali, il titolare del trattamento **notifica** la violazione **all'autorità di controllo** competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, **entro 72 ore** dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche

Security - L’importanza del Data Breach

La notifica di cui al paragrafo 1 deve almeno (art. 33):

a) **descrivere la natura della violazione dei dati personali** compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

b) **comunicare il nome e i dati di contatto del responsabile della protezione dei dati** o di altro punto di contatto presso cui ottenere più informazioni;

c) descrivere le **probabili conseguenze** della violazione dei dati personali;

d) descrivere le **misure adottate o di cui si propone l'adozione** da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Security - I costi del Data Breach

I principali costi della notifica al Garante per la Protezione dei dati personali in caso di Data Breach sono:

(1) Un avvicendamento anomalo di clienti

(2) Danni reputazione e diminuzione e perdita di fiducia dei clienti

(3) Attività di help desk

(4) Attività di internal investigation

(5) Spese legali

(6) Costi per il ripristino del sistema informativo

Reference: Ponemon Institute, Cost of Data Breach Study: Global Analysis, June 2016, Research financed by IBM, available at http://www-03.ibm.com/security/data-breach/

Security - Le eccezioni per la notifica del Data Breach

Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni (art. 34):

a) il titolare del trattamento ha messo in atto le **misure tecniche e organizzative adeguate** di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

b) il titolare del trattamento **ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato** per i diritti e le libertà degli interessati di cui al paragrafo 1;

c) **detta comunicazione richiederebbe sforzi sproporzionati**. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Security - Le misure tecniche-organizzative adeguate

Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo (art. 32).

ISO International Organization for Standardization

COBIT GOVERNANCE, CONTROL and ASSURANCE for INFORMATION and RELATED TECHNOLOGY

NIST National Institute of Standards and Technology U.S. Department of Commerce

Security - Gli organismi di certificazione

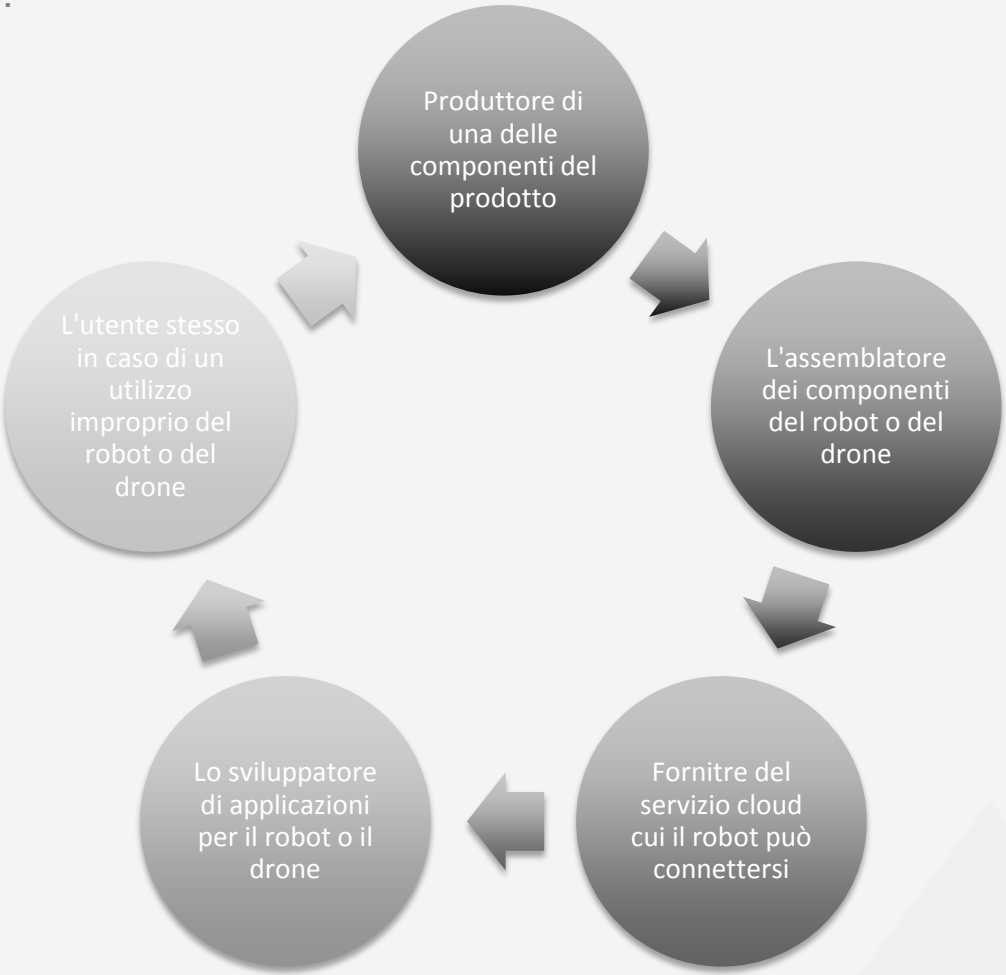
Gli Stati membri, le autorità di controllo, il comitato e la Commissione **incoraggiano, in particolare a livello di Unione, l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione** dei dati allo scopo di dimostrare la conformità al presente regolamento dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento.

Gli organismi di certificazione in possesso del livello adeguato di competenze riguardo alla protezione dei dati, **rilasciano e rinnovano la certificazione,** dopo averne informato l'autorità di controllo al fine di consentirne un'adeguata verifica

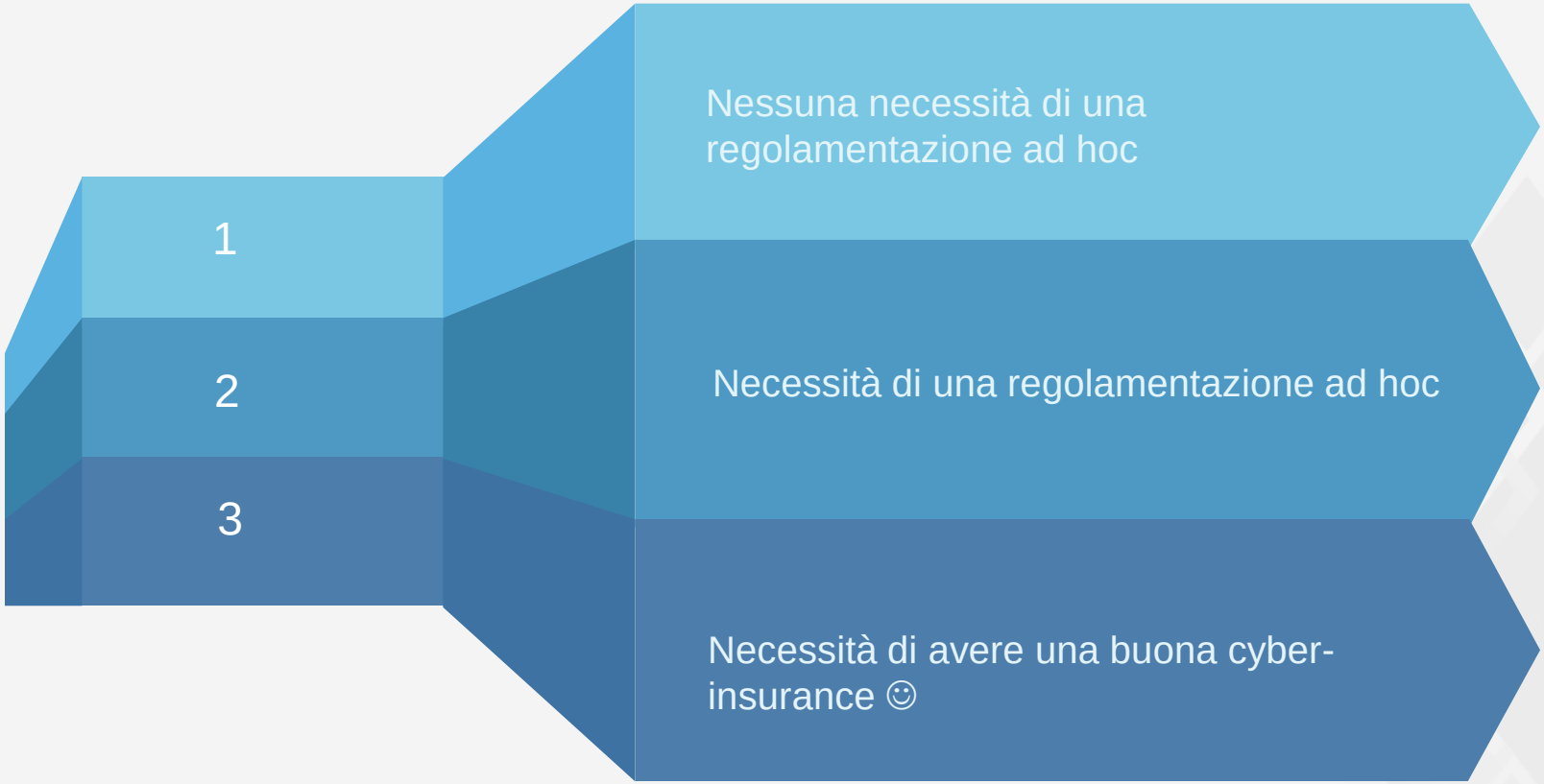
La conseguenza è che gli art. 34 e 42 del Regolamento Europeo sulla privacy potrebbe indurre le società che stanno investendo in robotica a implementare un adeguato sistema di standard e l'eventuale rispetto di un codice di condotta

Liability – L’allocazione delle responsabilità

Chi è il soggetto che deve garantire per la sicurezza di un device e che ne risponderà in caso di incidente?



Liability – 3 possibili scenari



Liability – Il framework normativo esistente

Esistono 4 principali direttive europee che potrebbero essere utilizzate per normare la robotica:

1. Direttiva 85/374/CE in tema di **responsabilità da prodotto**
2. Direttiva 2006/42/CE in tema di regolamentazione delle **macchine industriali**
3. Direttiva 2001/95/CE in tema di **sicurezza del prodotto**
4. Direttiva 1999/44/CE su taluni aspetti della **vendita e delle garanzie dei beni di consumo**

Il tema dell'allocazione delle responsabilità non riguarda solo la robotica o il mondo dell'IoT. Ciò che invece va regolato in modo più dettagliato sono le previsioni contrattuali che giocano un ruolo fondamentale in caso di incidente e conseguente allocazione delle responsabilità.

Reference: DIGITALEUROPE's, Views on the Internet of Things, Brussels, 14 April 2016, available at: http://goo.gl/ZNqOfC

Liability – Il framework normativo è carente

A livello Europeo vi sono alcuni autori che ritengono che soprattutto la Direttiva 85/374/CE in tema di responsabilità da prodotto e la Direttiva 31/00/CE in tema di commercio elettronico debbano essere riformate.

Reference: Commission Staff Working Document, Advancing the Internet of Things in Europe Accompanying the document, April 2016

A livello US, vi sono alcuni autori che invece addirittura sostengono che si dovrebbe ipotizzare una forma di esenzione di responsabilità per i provider di tali servizi esattamente come è stato ipotizzato nella Section 230 del Communications Decency Act del 1996 anche se è indubitabilmente più complesso trattandosi di beni materiali e non immateriali.
Reference: Ryan Calo, Robotics and the New Cyberlaw

Liability – Necessità di avere una Cyber-insurance

Le assicurazioni tradizionali corrono il rischio di trascurare molti aspetti critici per quanto attiene l'ambito cyber e quello della robotica. I contratti assicurativi in tale ambito dovranno essere valutati in modo molto attento e personalizzati.

Un aspetto da considerare e che emergerà nel prossimo futuro è sicuramente quello delle polizze è quello di definire chiaramente il perimetro di copertura verso l'assicurato e, soprattutto, in caso di responsabilità verso terzi

Una domanda interessante è quella dell'assicurabilità in caso di ransomware ove si sia deciso di pagare il riscatto

Reference: SGL Law Firm, The Internet of Things: a New Era of Cyber Liability and Insurance, January 2015

Digital Forensics – Preventiva o “by design”

Quali sono le possibili soluzioni per garantire una maggiore compliance in tema di digital forensics

1. Attenta policy in tema di mappatura degli asset delle fonti di prova digitale
2. Procedure di Incident Response che prevedano l'applicazione delle best practices di digital forensics

Mappatura (asset inventory) delle fonti di prova digitale

Fonte di prova	Tempi di conservazione	Luogo e modalità di conservazione	Copie di back up	Note
CCTV	**72** ore	Registrazione su server dedicato	No	Tempi di conservazione compliant con Garante Privacy
Log di accesso applicazione X	**6** mesi log in e log out	Registrazione su log server “xyz”	Si – Copie notturne registrazione su nastro	Tempi di conservazione compliant con Garante Privacy
	1 mese log in utenti generici	Registrazione in locale su application server	No	

Digital Forensics – Reattiva o “post-mortem”

In linea teorica, l’industry 4.0 genererà un incredibile numero di dati personali e sensibili. In questo nuovo scenario, ci sarà anche il rischio che le prove digitali possano essere contradditorie tra di loro. Al di là di questa considerazione le sfide legali e tecniche della digital forensics sono:

1. **Fase di identificazione**: Cloud e giurisdizione
2. **Fase di acquisizione**: Cloud e giurisdizione
3. **Fase di analisi**: formato proprietario e varietà di device da analizzare
4. **Presentazione**: i device potrebbero contenere sempre meno dati utili ai fini della digital forensics

Reference: R.C.Hegarty, D.J.Lamb and A.Attwood, Digital Evidence Challenges in the Internet of Things (2013)

Le sfide di policy

Settore pubblico-privato

Focus sul consumatore

Focus sul settore privato

Frammentazione internazionale e definizione delle norme

Deficit di fiducia tra governo e settore privato

Tutela della privacy = tutela della sicurezza: la qualità del consenso del consumatore

Mancanza del controllo e asimmetria dell'informazione

Inadeguatezza delle attuali strutture nella condivisione dell'informazione

Disallineamento degli incentivi per la buona pratica della cybersicurezza

I. Frammentazione internazionale e definizione delle norme

La frammentazione a livello internazionale

Diversi approcci alla cybersicurezza, alla giurisdizione dei dati e all'applicazione del diritto attraverso i confini territoriali e giurisdizionali possono rendere difficile prevenire, indagare e perseguire in modo efficace.

La definizione delle norme a livello internazionale

Le differenze di politiche a livello internazionale e gli specifici programmi di ciascun paese rendono complesso lo sviluppo di una normativa condivisa riguardante la cybersicurezza, ancor più l'esecuzione di essa.

Reference: World Economic Forum, Global Agenda Council on Cybersecurity, April 2016

II. Deficit di fiducia tra governo e settore privato

Il deficit di fiducia ostruisce qualsiasi tipo di collaborazione, creando preoccupazione per l'esattezza delle informazioni condivise.

III. Tutela della privacy = tutela della sicurezza: la qualità del consenso del consumatore

È necessario considerare nuovi metodi per ottenere un valido consenso dell'utente, includendo meccanismi di consenso che funzionino attraverso gli stessi dispositivi.

IV. Mancanza del controllo e asimmetria dell’informazione

L'interazione tra i diversi soggetti (oggetti, dispositivi, individui) crea flussi di dati difficili da gestire con gli strumenti tradizionali, insufficienti ad assicurare una protezione adeguata dei diritti e degli interessi dei soggetti.

V. Inadeguatezza delle attuali strutture nella condivisione dell'informazione

Deficit di fiducia, obblighi di segretezza, strutture inefficienti per la condivisione e la responsabilità dei rischi vincolano e limitano la condivisione.

VI. Disallineamento degli incentivi per la buona pratica della cybersicurezza

Le aziende si trovano in difficoltà nel dover bilanciare da una parte la pressione del mercato dovuta alla rapidità dell'innovazione dall'altra gli investimenti sostenibili nella cybersicurezza, questo potrebbe far lievitare i costi oppure ritardare il lancio dei prodotti nel mercato.

La vera sfida è massimizzare l’efficacia degli interventi governativi bilanciando gli obiettivi di sicurezza con una innovazione efficiente.

Possibili soluzioni

Legal – Standardizzazione

C’è una grande richiesta a livello internazionale di standard, interoperabilità, APIs, data sharing e soprattutto in tema di protezione dei dati personali

EU: Commission Staff Working Document, Advancing the Internet of Things in Europe Accompanying the document, April 2016

FTC: FTC Staff Report, The Internet of Things: Privacy and Security in a Connected World, January 2015

OFCOM: OFCOM (Communications Regulator in the UK),

Promoting investment and innovation in the Internet of Things, January 2015, Ministry of Communication and IT of India: Department of Electronics & Information

Technology, Draft Policy on Internet of Things, 2014

Politecno di Milano: Osservatorio sull'Internet of Things del Politecnico di Milano "L'Internet of Things in Italia: Stato dell’arte e trend di mercato", June 2015

Legal – Privacy Impact Assessment (PIA)

Privacy Impact Assessment (PIA) è un processo di **analisi del rischio** finalizzato ad un assessment degli impatti in termini di **privacy e security di un determinato device** che sia IoT o Robotics nell'ottica di prendere le opportune azioni al fine di prevenire o minimizzare tali impatti

Il PIA report è il documento di sintesi dell'analisi e dell'assessment che deve essere reso disponibile alle autorità competenti.

Benefici:

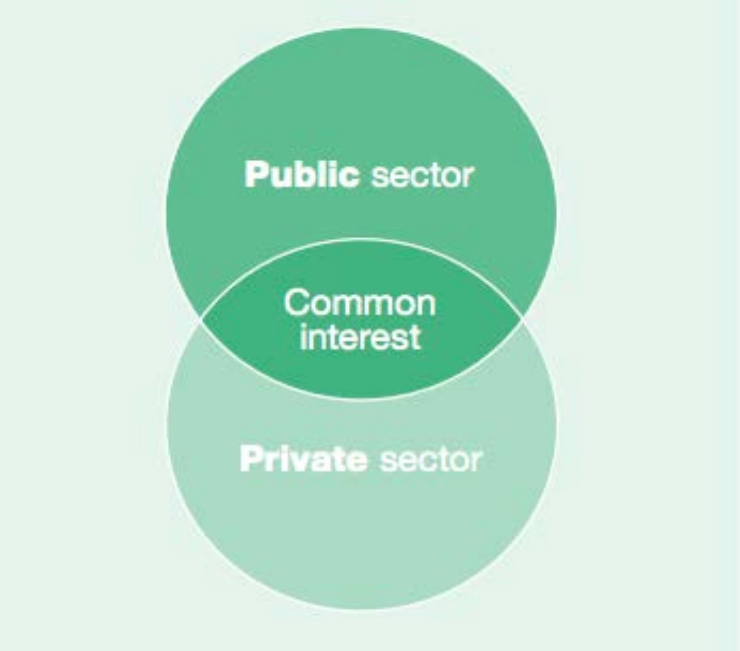
- Eliminare il rischio associato al trattamento dei dati
- Costruire fiducia con chi usa i loro servizi
- Vantaggi finanziari
- Aumenta la consapevolezza per la privacy dell'azienda e dei dipendenti

Legal – Data Minimization

Le società che raccolgono dati personali dovrebbero seguire il principio della data minimization, ossia quello di raccogliere solo i dati necessari per una finalità specifica per poi cancellarli in modo sicuro dopo l'utilizzo

Policy – Blended Governance

È necessario sperimentare nuovi paradigmi per una governance collaborativa che consentano di indirizzare le nuove sfide della security sia al mondo pubblico che a quello privato.



Policy – Privacy and Security Risk Assessment

Le società dovrebbero condurre con maggiore continuità e frequenza risk assessment finalizzati a monitorare i processi sul prodotto e ad eliminare le possibili vulnerabilità

Esse dovrebbero:

- monitorare tutto il ciclo di vita del prodotto
- aggiornare le vulnerabilità note (per quanto è possibile)

Policy – Security, Privacy and Safety by Design

I principi in tema di Security, Privacy and Safety by Design devono essere seguiti e adattati ai vari contesti in cui viene realizzato il prodotto.

Ad esempio, se una rete che monitora un campo minato è compromessa, la sicurezza delle persone è la prima priorità. Se una smart-home è compromessa, la principale preoccupazione sarà la privacy delle persone che abitano in quella casa.

Un possibile principio per la progettazione potrebbe essere la disabilitazione automatica dei dispositivi che raccolgono le informazioni più sensibili quando viene rilevata un'intrusione (ad esempio: disabilitare alcuni sensori non appena la rete è sotto attacco).

Conclusioni

Regolamentare o non regolamentare?

“Well, I have to tell you that regulation is tricky. And I don’t know, if somebody asked me, would you write a regulation for this, I would not know what to say. I don’t think I have enough understanding of all of the cases that might arise in order to say something useful about this, which is why I believe we are going to end up having to experience problems before we understand the nature of the problems and maybe even the nature of the solutions”

Remarks of Cerf, Transcript of Workshop, FTC Report on Internet of Things

Il ruolo del Regolamento Europeo

Il Regolamento Europeo è un esperimento unico nel panorama legislativo europeo: una normativa direttamente applicabile a tutti gli Stati Membri che impone alcune regole e principi fondamentali in ambito security con un impatto rilevante anche nel settore della robotica e della AI. Nello specifico:

1. Privacy by Design
2. Rispetto di standard di sicurezza
3. Data Breach
4. Privacy Impact Assessment

Tuttavia, i punti di debolezza non mancano:

1. le società extra UE che non trattano i dati UE non devono rispettare tale normativa (si pensi ai produttori di device di robotica ad esempio).
2. L'incentivo per rispettare gli standard di sicurezza, ossia la possibilità di evitare la notifica all'interessato in caso di data breach, potrebbe non essere sufficiente.

Sicuramente però, il Regolamento Europeo è un ottimo punto di partenza….

Contact Us

Tech and Law Center

www.techandlaw.net

info@techandlaw.net

twitter.com/techlawcenter

facebook.com/techandlawcenter