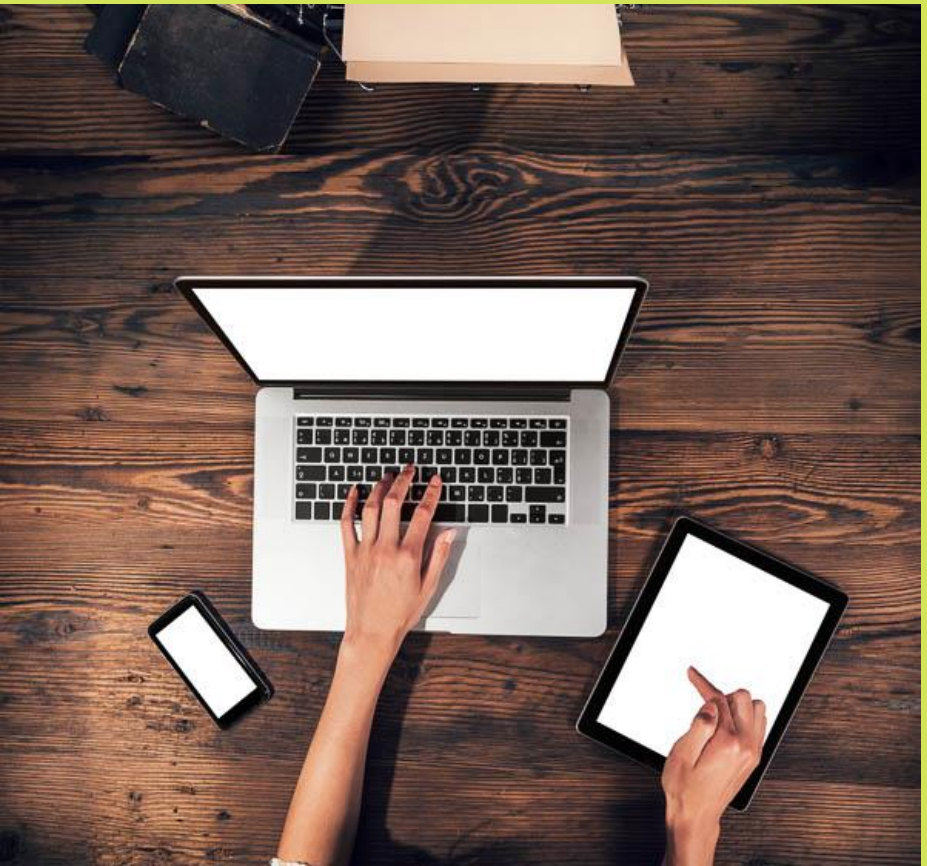
Rödl & Partner

INTERNAZIONALIZZAZIONE 4.0 - ANALISI GIURIDICA DEGLI STRUMENTI DIGITALI PER RILANCIARE L'IMPRESA SUI MERCATI ESTERI



Terzo Incontro_After Sales

18.06.2020, Confindustria Lombardia

Relatori:

Avv. Eugenio Bettella, Managing Partner Rödl & Partner

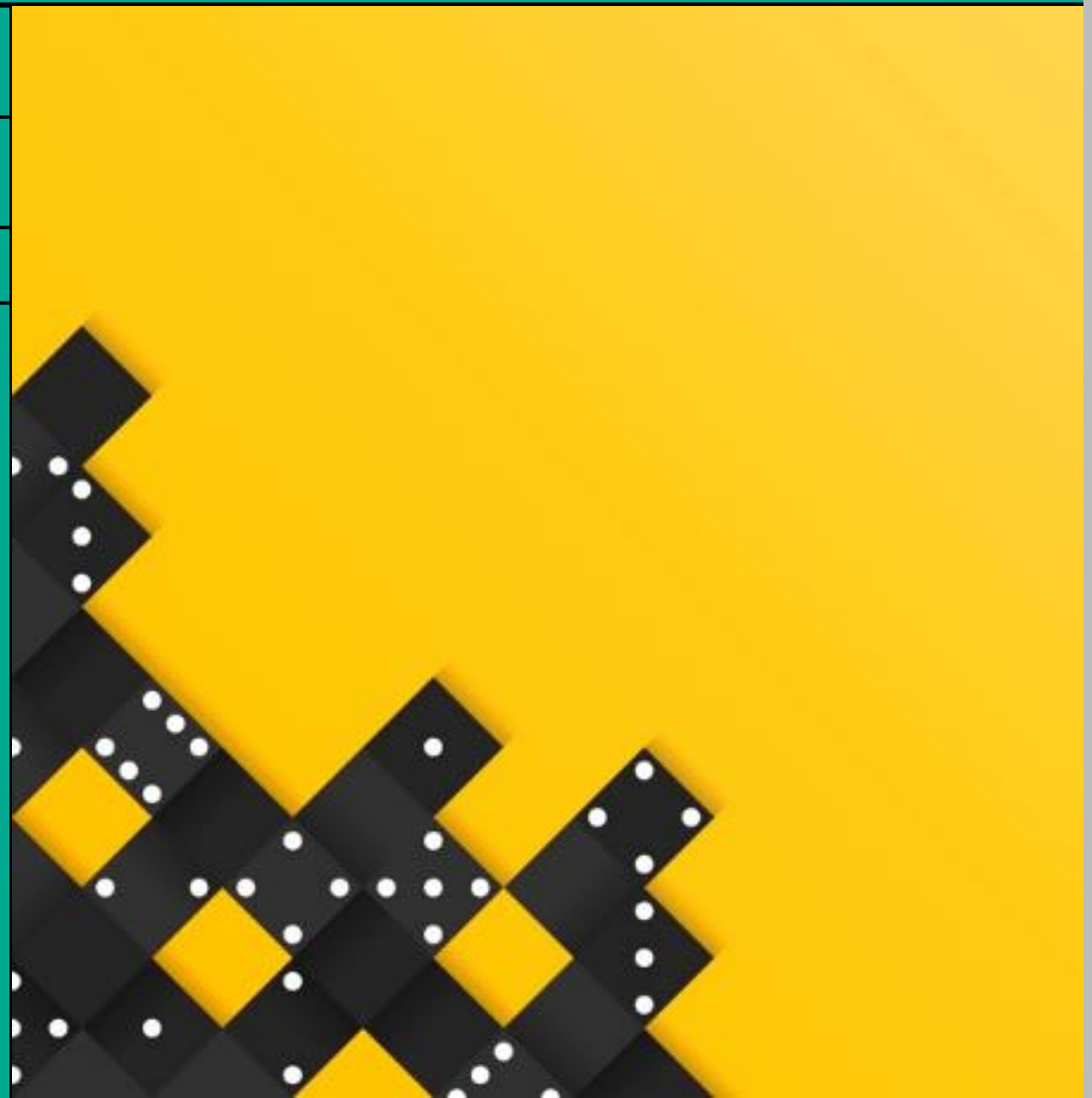
Avv. Giuliana Viviano, Associate Partner Rödl & Partner

Avv. Margherita Cera, Associate Rödl & Partner

CONFINDUSTRIA Lombardia

AGENDA

1. **IOT E IA PER L'*AFTER SALE*
QUADRO NORMATIVO DI RIFERIMENTO**
2. **PROBLEMATICHE GIURIDICHE
DELL'*IoT* E DELL'*IA***
3. **APPROFONDIMENTI IN TEMA DI TUTELE ASSICURATIVE**



1. IOT E IA PER L'AFTER SALE
QUADRO NORMATIVO DI RIFERIMENTO

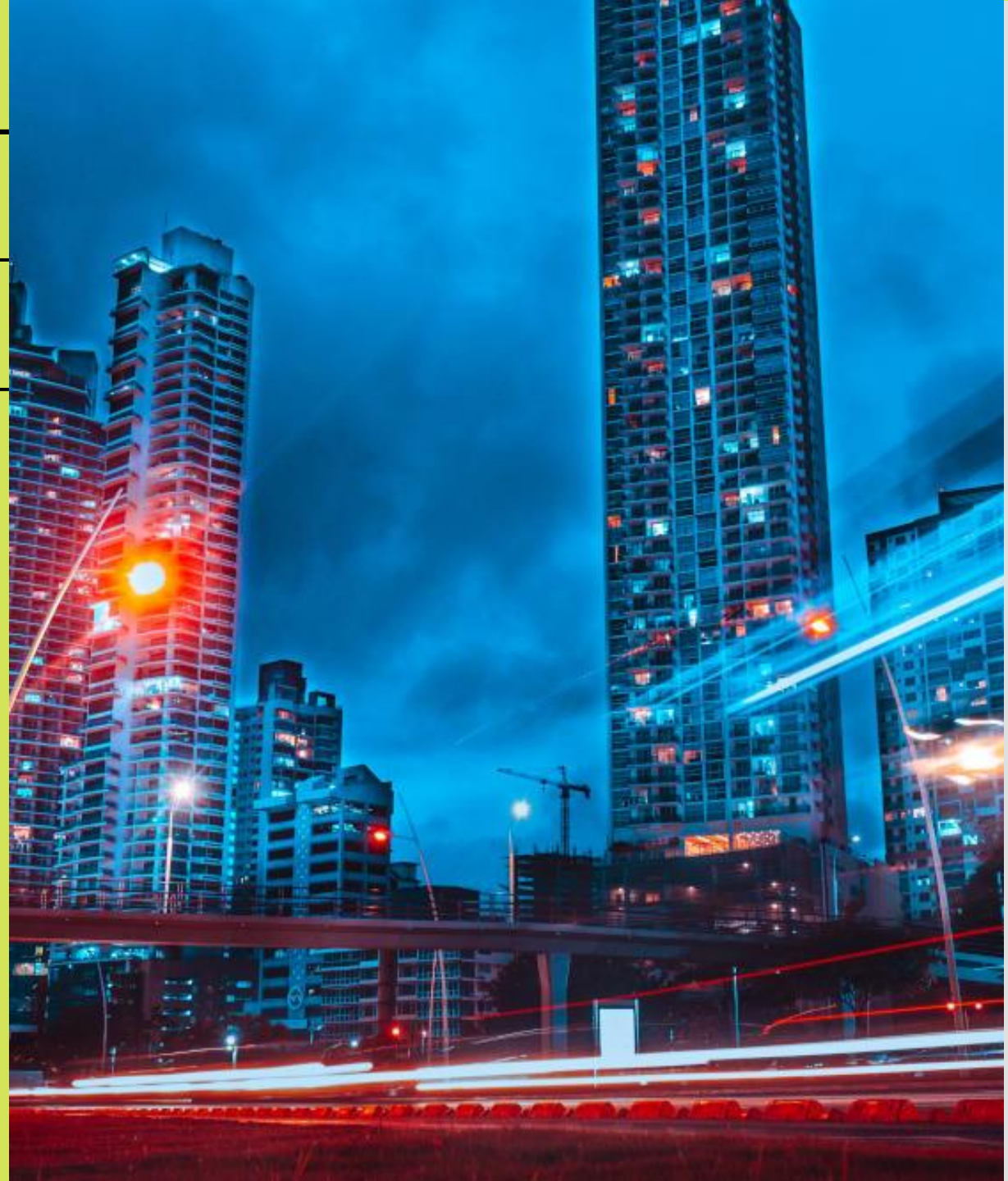
1.1 **IoT e IA per assistenza post vendita e remote customer care**

1.2 *IoT* e *IA*: quadro giuridico di riferimento

Relatore:

Avv. Eugenio Bettella,

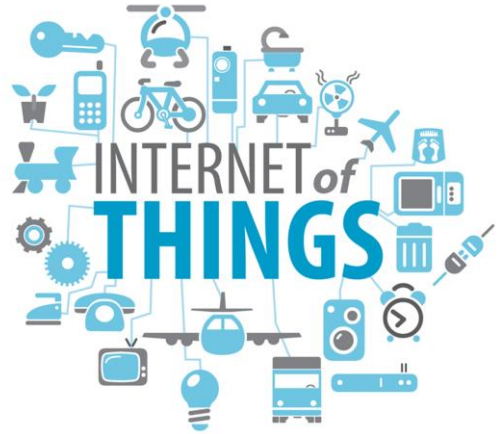
Managing Partner Rödl & Partner



INTERNET OF THINGS (I.o.T.)

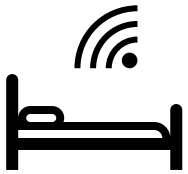
*«oggetti che dispongono del proprio **indirizzo IP**, utilizzano **sensori per ottenere informazioni** dal proprio ambiente e/o **dispositivi di comando** per interagire con lo stesso»*

Comunicazione della Commissione al Parlamento Europeo del 18/06/2009



1.1 *IoT e IA* per assistenza post vendita e remote customer care

ESEMPI DI *INTERNET OF THINGS*



Home Automation

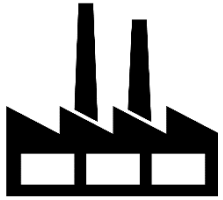
applicazioni a scopo di *security* (videosorveglianza, antintrusione), di manutenzione impianti (rilevazione guasti, gestione della manutenzione) e di "gestione scenari" (climatizzazione, illuminazione, irrigazione).

Smart Cities

sono capaci di raccogliere dati in tempo reale da sensori e dispositivi, per poi integrarli e renderli accessibile ai vari fornitori di servizi urbani, per ottimizzarne la fornitura.

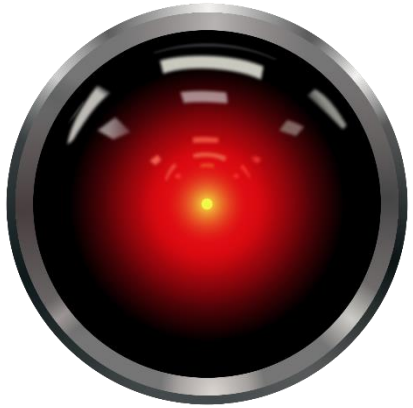
Smart Car

Consentono la manutenzione preventiva e l'integrazione degli *smart speaker*.



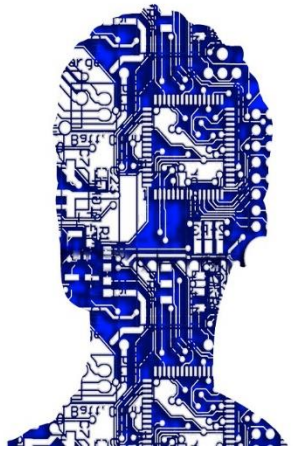
Smart factory

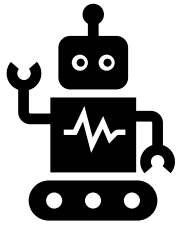
Impresa che ha implementato sistemi automatizzati e intelligenti, che operano in maniera autonoma e in contatto con l'ambiente circostante.



INTELLIGENZA ARTIFICIALE (IA)

*«**sistemi** che mostrano un **comportamento intelligente** analizzando il proprio ambiente e compiendo azioni, per raggiungere specifici obiettivi. I sistemi basati sull'IA possono consistere in **software che agiscono nel mondo virtuale** (ad esempio software per l'analisi delle immagini, motori di ricerca, ecc.), oppure incorporare l'**IA in dispositivi hardware** (per esempio in robot avanzati, auto a guida autonoma, droni o applicazioni dell'Internet delle cose)»*





Comunicazione della Commissione al Parlamento europeo, del 25 aprile 2018.

1.1 *IoT e IA* per assistenza post vendita e remote customer care

IoT e **IA** abilitano la cosiddetta «**SERVITIZATION**», una logica relazionale che mira alla fornitura non solo di un prodotto ma anche dei cosiddetti «***SMART SERVICES***» nella fase post vendita.

GLI STRUMENTI DEL PROCESSO DI *AFTER SALE* DIGITALIZZATO

LA PIATTAFORMA ONLINE DELL'IMPRESA PER IL CUSTOMER CARE

APP PER DIALOGO IMPRESA E CLIENTE

DISPOSITIVO INTELLIGENTE PER CONTROLLO DA REMOTO

I DISPOSITIVI INTELLIGENTI consentono di soddisfare più compiutamente i 4 ambiti di azione del servizio post-vendita, ossia: (i) installazione del prodotto; (ii) assistenza in garanzia o non in garanzia; (iii) gestione dei ricambi; (iv) upgrade del prodotto.

IL FATTORE CHIAVE

La **connettività dell'IoT e l'IA** consentono al prodotto di interagire con l'impresa e, quindi, di fornire informazioni in relazione alla *performance* del prodotto per un rapido intervento dell'impresa anche in forma predittiva, rispetto a malfunzionamenti o aggiornamenti.

I VANTAGGI DELLA *SERVITIZATION* PER l'INTERNAZIONALIZZAZIONE

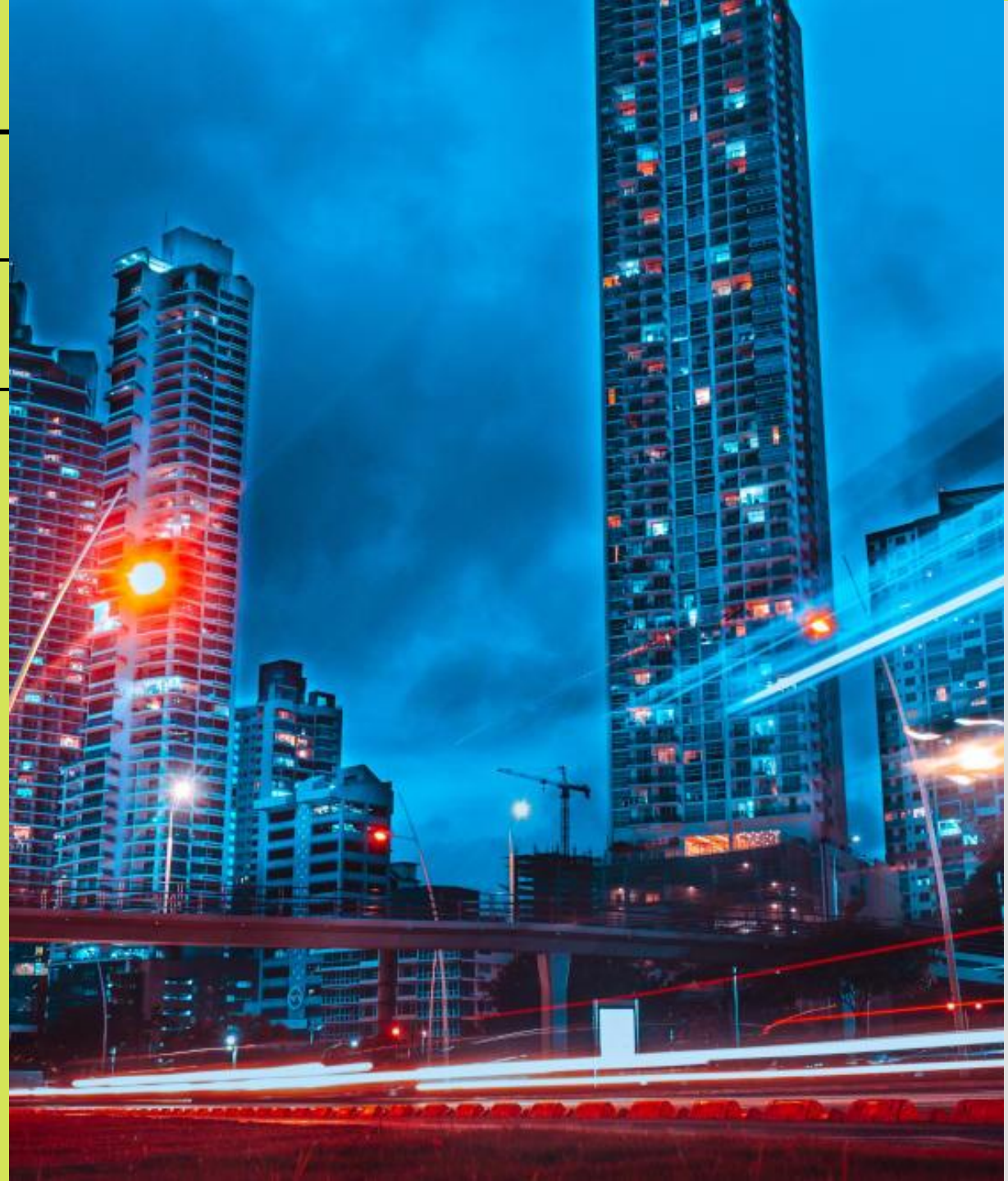
Servitization
How it matters

- AZZERAMENTO DELLA DISTANZA CON IL CLIENTE ESTERO.
- ELIMINAZIONE DI INTERMEDIARI COME CENTRI DI ASSISTENZA O TECNICI MANUTENTORI.
- MIGLIORE COMPRENSIONE DEL PRODOTTO PER LO STUDIO DI VERSIONI PERFEZIONATE.

1. IOT E IA PER L'AFTER SALE
QUADRO NORMATIVO DI RIFERIMENTO

1.1 IoT e IA per assistenza post vendita e remote customer care

1.2 **IoT e IA: quadro giuridico di riferimento**



NON C'E' UNA NORMATIVA AD HOC PER I DISPOSITIVI INTELLIGENTI.

Il giurista e con esso l'impresa è chiamato ad analizzare il fenomeno tecnico sociale incanalandolo, irregimentandolo e gestendolo in base alla normativa preesistente.

1.2 IoT e IA: quadro giuridico di riferimento in UE e Italia

I tre *framework* normativi da tenere in considerazione

RESPONSABILITÀ DEL PRODUTTORE

- Dir. 2001/95/CE sulla sicurezza dei prodotti;
- Dir. 2006/42/CE relativa alla macchine;
- Dir. 1999/44/CE sulle garanzie dei beni di consumo;
- Dir. 2011/83/UE sui diritti dei consumatori;
- Codice del Consumo.

SOFT LAW SPECIFICA

- Linee guida della Commissione Europea dell'8 aprile 2019 per una IA affidabile.
- Linee guida ENISA per la sicurezza dell'IoT aziendale del 19 novembre 2018.

PRIVACY E CYBERSECURITY

- Normativa UE e Italiana in tema di privacy e cybersecurity, e relativi provvedimenti delle autorità nazionali.

2. PROBLEMATICHE GIURIDICHE DELL'IOT E DELL'IA

2.1 **Trattamento e protezione dei dati personali dei trasmessi attraverso i dispostivi intelligenti**

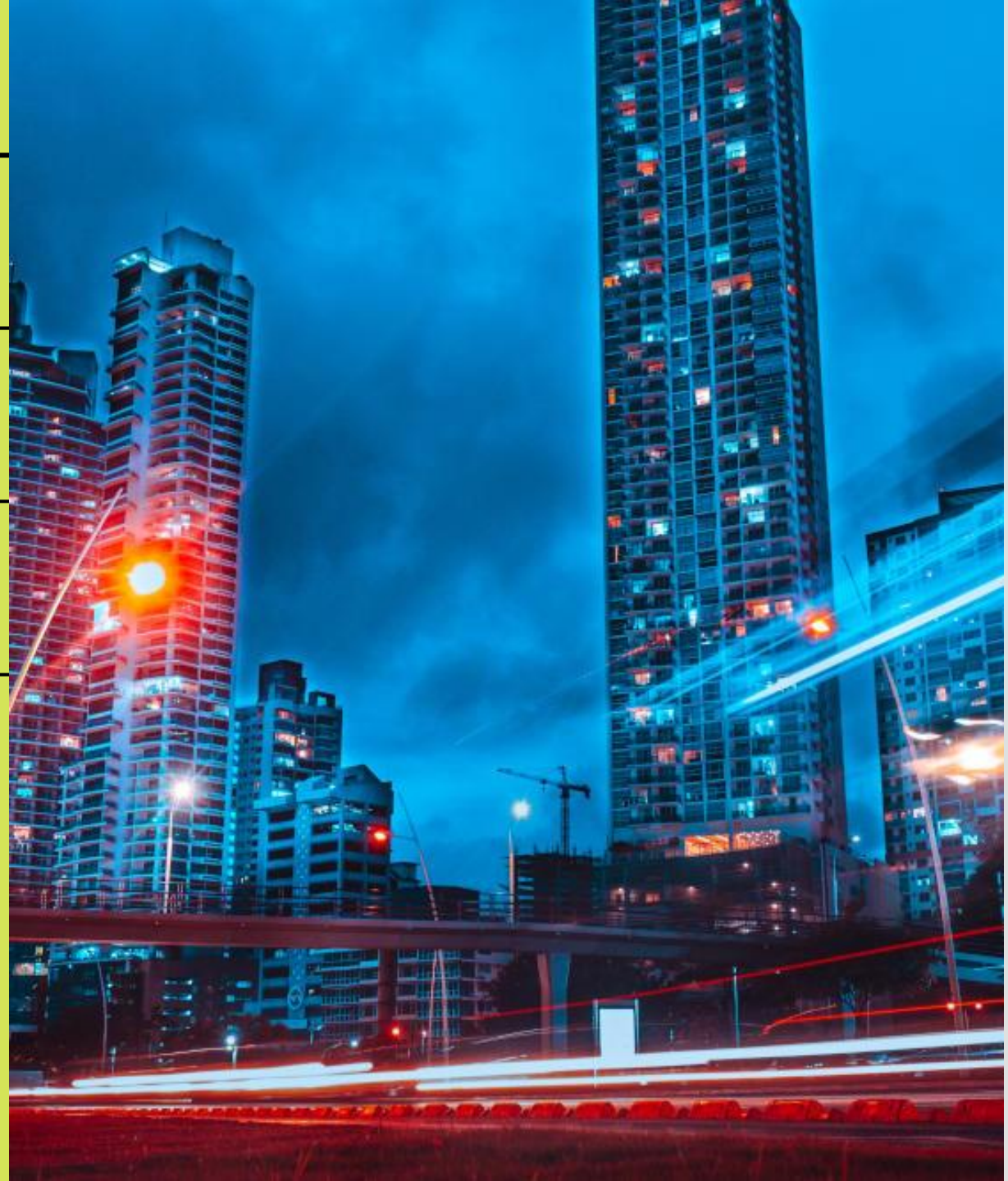
2.2 Assistenza post vendita e *remote customer care* digitalizzata: modelli contrattuali e clausole tipiche

2.3 Responsabilità civile per malfunzionamento dei dispositivi intelligenti

Relatore:

Avv. Giuliana Viviano,

Associate Partner Rödl & Partner



2.1 Focus su normativa in tema di privacy e cybersecurity

- **Il GDPR**
- **Il Codice in materia di protezione dei dati personali (D. lgs. del 30 giugno 2003, n. 196) come modificato dal Decreto legislativo 10 agosto 2018, n. 101;**
- **I provvedimenti del Garante compatibili il GDPR;**
- **D. lgs n. 65/2018 di recepimento della direttiva NIS;**
- **Decreto-legge n.105 del 2019 in materia di perimetro di sicurezza nazionale cibernetica come modificato dal Decreto c.d. «Milleproroghe"**

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Hai avviato un adeguato progetto di risk assessment sin dalla progettazione dell'IoT?

Le imprese devono valutare le problematiche privacy già in **fase di progettazione** dei dispositivi intelligenti per attuare in modo efficace i principi di protezione dei dati, quali in *primis* la minimizzazione – **art. 25 GDPR**

2.1 Focus su normativa in tema di privacy e cybersecurity – i principi da rispettare

Qual è la base giuridica del trattamento che stai effettuando?

Hai predisposto un'adeguata informativa?

I dati personali raccolti tramite dispostivi intelligenti devono essere raccolti per **finalità determinate, esplicite e legittime**, devono essere "*adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati*" e, infine, conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità del trattamento – **ART. 5 GDPR**

2.1 Focus su normativa in tema di privacy e cybersecurity – i principi da rispettare

Hai studiato delle procedure per la gestione degli eventuali data breach?

Hai implementato delle adeguate misure di sicurezza nel tuo Iot?

Il titolare del trattamento e il responsabile del trattamento devono mettere in atto **misure tecniche e organizzative adeguate** per garantire la **sicurezza** del trattamento dei dati personali raccolti con il dispositivo intelligente – **ART. 32 GDPR**

IL PROSSIMO FUTURO:
LA CERTIFICAZIONE DEI DISPOSITIVI INTELLIGENTI!

Considerando 65 del *CYBERSECURITY ACT*:

«*La **certificazione della cibersicurezza** riveste un **ruolo importante** nel rafforzare la sicurezza di prodotti TIC, servizi TIC e processi TIC e nell'accrescere la fiducia negli stessi. Il mercato unico digitale, in particolare l'**Internet degli oggetti**, possono prosperare solo se i cittadini sono convinti che tali prodotti, servizi e processi offrono un **determinato livello di cibersicurezza***».

COSA PREVEDE IL *CYBERSECURITY ACT* IN MATERIA DI PREVENZIONE : APPROCCI GENERALI

Il *Cybersecurity Act* (Reg. UE 881/2019) ha evidenziato alcuni **importanti principi** per una **corretta strategia** di cibersicurezza :

- "***cyber-hygiene***". In materia di *cybersecurity* il comportamento umano è importante tanto quanto il fattore tecnologico. L'utente è chiamato ad adottare semplici **comportamenti di routine** (ad es. frequenti cambi password) che se svolti regolarmente consentono di **ridurre al minimo** l'esposizione a **rischi** derivanti da minacce informatiche.
- "***security by design***" e "***security by default***". Le imprese devono garantire che i dispositivi e le infrastrutture informatiche siano progettati fin dall'inizio con le **più elevate misure di sicurezza possibili** (*security by design*), riducendo al contempo l'onere in capo all'utente di dover configurare il *device* in modo adeguato (*security by default*).

RISCHI INFORMATICI. NUOVE MINACCE ED ATTACCHI AI TEMPI DEL COVID-19

Di recente l'ENISA ha evidenziato che da fine febbraio ad oggi, i casi di ***phishing*** sono aumentati più del **600%** per gli effetti del Covid-19 (1).

I criminali informatici **sfruttano** la forte **sensibilità pubblica** che circonda il tema "Coronavirus" per portare a segno **attacchi mirati** a danno di ignari cittadini.

Queste frodi informatiche comportano importanti riflessi non solo in materia di ***smart working,*** ma anche per la sicurezza **dei servizi IoT forniti dall'impresa**.
Infatti, se questi attacchi si verificano nei confronti di un pc aziendale o di dispositivo personale utilizzato dal dipendente per svolgere l'attività lavorativa da remoto (**BYOD**), vi è il concreto rischio che i criminali informatici possano avere **accesso** non solo alle informazioni personali dell'utente ma anche ai **dati aziendali** della società, **relativi anche ai software e ai servizi IoT** che l'impresa offre e/o gestisce, compromettendone la sicurezza.

(1) ENISA, *Understanding and dealing with phishing during the covid-19 pandemic,* 6 Maggio 2019, https://www.enisa.europa.eu/

2.1 Focus su normativa in tema di privacy e cybersecurity -TRUFFE *ONLINE*

TIPOLOGIA	SPIEGAZIONE
• DDoS;	richieste reiterate verso un sito, fino a metterlo ko e renderlo irraggiungibile.
• Phishing	truffe in cui l'hacker cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile.
• Malware	programma informatico usato dai cyber-criminali solitamente per entrare in possesso di informazioni sensibili, accedere a sistemi informatici privati o mostrare pubblicità indesiderata
• Ramsonware	malware specificatamente progettati a scopo di ricatto (estorsione).

I consigli del Garante per la protezione dei dati personali per evitare le truffe

1. posizionare sempre il puntatore del mouse sui link prima di cliccare: in molti casi si potrà così leggere in basso a sinistra nel browser il vero nome del sito cui si verrà indirizzati.

2. E' utile prestare attenzione al mittente (che potrebbe avere un nome vistosamente strano o eccentrico) o al suo indirizzo di posta elettronica (che spesso appare un'evidente imitazione di quelli reali).

3. Non memorizzare dati personali e codici di accesso nei browser utilizzati per navigare online.

4. Effettuare back up periodici dei contenuti per evitare che vadano persi in un attacco.

5. Mai pagare il riscatto richiesto in caso di attacco malware: lo sblocco potrebbe non avvenire mai e vi sarebbe oltretutto una perdita di reputazione dell'impresa.

2.1 Focus su normativa in tema di privacy e cybersecurity

INTERVENTI PRATICI IN MATERIA DI CYBERSECURITY

l'ENISA ha stilato per le piccole e medie imprese alcuni consigli tecnici di «***cyber-hygiene***» mirati alla prevenzione dei rischi informatici e alla protezione degli *asset* digitali (2) :

- **Aggiornare** i regolamenti e le ***policy* aziendali** in materia di *cybersecurity;*
- **Risk Assessement** dei principali rischi cyber (e non);
- **Informare** i lavoratori sui pericoli connessi allo **smart working;**
- **Incident management plan,** predisporre un piano per la gestione degli incidenti informatici;
- **Rafforzare** la generale **sicurezza** delle reti infrastrutturali:
  - **Aggiornare** costantemente **antivirus** e **strumenti di lavoro** (server, workstation, smartphone aziendali ecc.);
  - Utilizzare **VPN** (*Virtual Private Network*s) per mantenere privata la connessione alla rete aziendale;
  - Garantire sistemi di acceso a **doppia autenticazione**, 2FA (*two factor authentication*);
  - Effettuare costanti **back up** dei dati.

(2) ENISA, *Top ten cyber hygiene tips for SMEs during covid-19 pandemic*, 2 giugno 2020, https://www.enisa.europa.eu/

2.1 Focus su normativa in tema di privacy e cybersecurity - le certificazioni

In attesa degli standard certificativi emanati dall'ENISA in base al *Cybersecurity Act*, si possono considerare gli standard relativi all'IoT stabiliti a inizio 2019 dall'ISO –, con il documento "***ISO/TR 22100-4:2018, Safety of Machinery – Relationship with ISO 12100 – Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects***".

2. PROBLEMATICHE GIURIDICHE DELL'IOT E DELL'IA

2.1 Trattamento e protezione dei dati personali dei trasmessi attraverso i dispostivi intelligenti

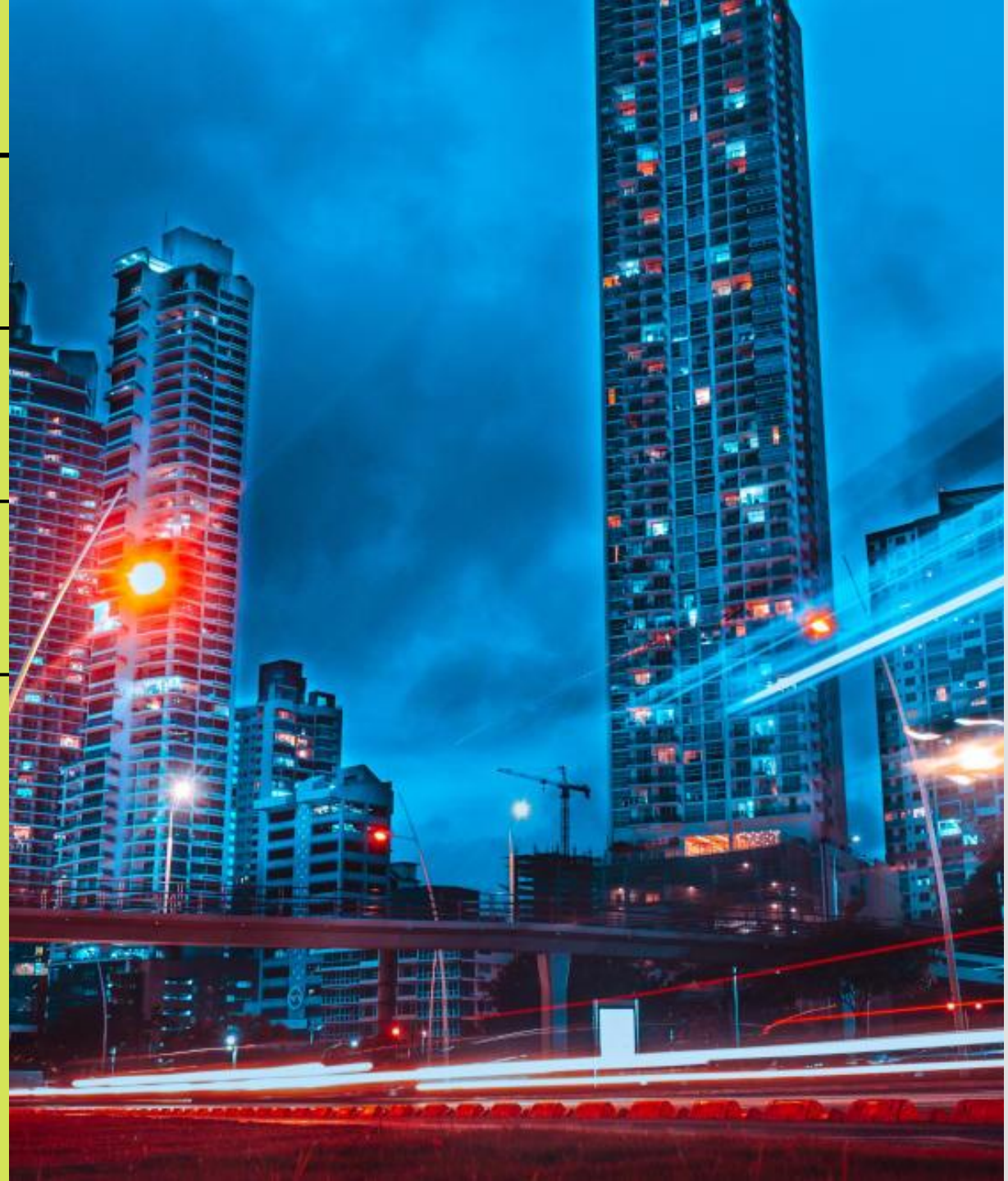
2.2 **Assistenza post vendita e *remote customer care* digitalizzata: modelli contrattuali e clausole tipiche**

2.3 Responsabilità civile per malfunzionamento dei dispositivi intelligenti

Relatore:

Avv. Margherita Cera,

Associate Rödl & Partner



2.2 Assistenza post vendita e *remote customer care* digitalizzata: modelli contrattuali

DISPOSITIVO COME PRODOTTO

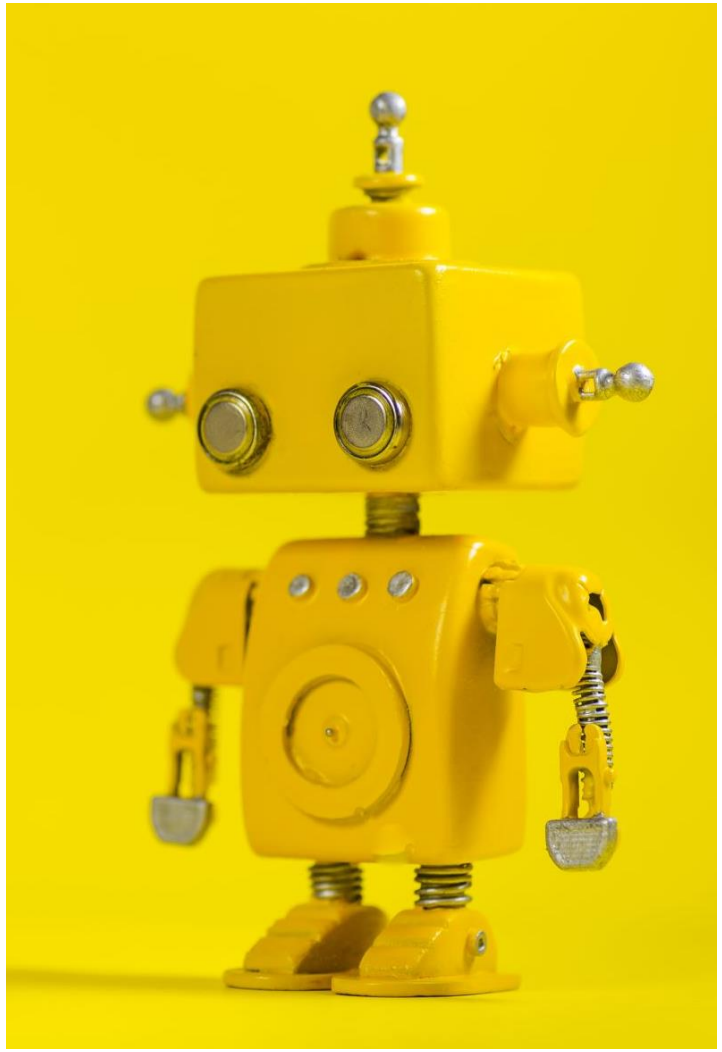
Il supporto fisico del dispositivo intelligente è un prodotto oggetto di un apposito contratto di compravendita.

Attenzione al **PROBLEMA DELLE GARANZIE**!

DISPOSITIVO COME SERVIZIO

Il dispositivo dà accesso a una rete di servizi attraverso l'uso di App

- **contratto [illegible]iluppo di App;**
- **contratto di licenza di App.**



IL CONTRATTO PER LO SVILUPPO / LA LICENZA DI UN ALGORITMO DI MACHINE LEARNING

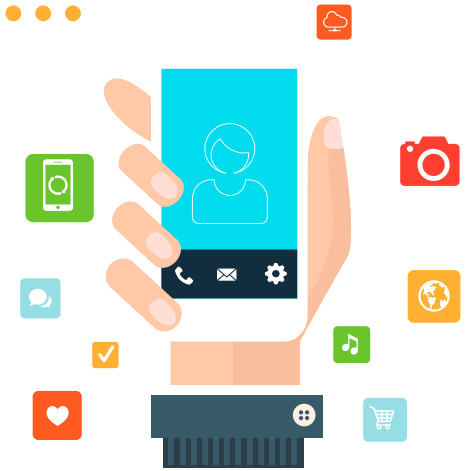
- Con il Contratto di Sviluppo di un algoritmo di *machine learning* l'impresa affida ad un fornitore – una software house o un professionista - la realizzazione di un algoritmo di machine learning di cui l'impresa diverrà titolare esclusiva

- Con il Contratto di licenza di un algoritmo di *machine learning* il titolare dei diritti di sfruttamento economico di quell'algoritmo, concede all'impresa la possibilità di usarlo in via esclusiva o non esclusiva, a tempo determinato o indeterminato per scopi predefiniti.

- È importante che l'impresa si tuteli nei confronti del titolare dell'algoritmo per il caso di difetti (manleva + assicurazione)

- Nell'ordinamento italiano non esiste una tipologia di contratto specifica ad hoc che ricade quindi nella categoria dei contratti per la realizzazione di opere intellettuali.

2.2 Assistenza post vendita e *remote customer care* digitalizzata: modelli contrattuali



IL CONTRATTO PER LO SVILUPPO DI UNA APP DI ASSISTENZA POST VENDITA

- Con il Contratto di Sviluppo App l'impresa affida ad un fornitore – una software house o un professionista - la realizzazione di programmi per fornire assistenza post vendita da remoto in cambio di un corrispettivo.

- Nell'ordinamento italiano non esiste una tipologia di contratto specifica ad hoc che ricade quindi nella categoria dei contratti per la realizzazione di opere intellettuali.

LE CONDIZIONI GENERALI DI UTILIZZO DELL'APP

- Rappresentano il *digital contract* tipicamente utilizzato per regolare il rapporto di utilizzo dell'App da parte della clientela B2B e B2C.

- La conclusione avviene tramite il **meccanismo di «point&click»** presente sul sito web dell'impresa ovvero sul web store gestita da una piattaforma terza (ad es. *google play*).

- Valgono i consigli già spiegati per le condizioni generali per l'*e-commerce*:
  - ➢ l'impresa deve prevedere il **download** delle condizioni generali per soddisfare il requisito di conoscibilità ex art. 1341 Cod. Civ.;
  - ➢ E' consigliabile predisporre, un **tasto ad hoc**, e richiedere un login con digitazione username e pwd per l'accettazione delle **clausole vessatorie**.

2.2 FIRMA ELETTRONICA

LE FONTI NORMATIVE IN UE E ITALIA

- Il **Regolamento eIDAS** (*electronic IDentification Authentication and Signature*) - Regolamento UE n° 910/2014 sull'identità digitale.

- **Codice dell'Amministrazione Digitale** (**CAD**) - decreto legislativo 7 marzo 2005, n. 82.

LE TIPOLOGIE DI FIRMA ELETTRONICA

- **Firma Elettronica semplice**: insieme di dati in forma elettronica, connessi ad altri dati elettronici, utilizzati come metodo di identificazione informatica – esempio: password mail, firma scannerizzata.

- **Firma elettronica avanzata**: insieme di dati in forma elettronica che consentono l'identificazione del firmatario del documento - esempio: firma grafometrica su tablet.

- **Firma elettronica qualificata**: tipo particolare di firma elettronica avanzata basata su dispositivo sicuro per la creazione della firma - esempio: smart card.

- **Firma digitale:** tipo particolare di firma elettronica avanzata basata su un sistema di chiavi crittografiche pubblica e privata– esempio: firma digitale avvocati.

L'EFFICACIA PROBATORIA DELLA FIRMA ELETTRONICA
ART. 20 CAD

I documenti con firma elettronica avanzata, firma elettronica qualificata, firma digitale, hanno la medesima **efficacia probatoria prevista dall'art. 2702 C.C.** per le scritture private.

I documenti con firma elettronica semplice sono **liberamente valutabili dal giudice**, tenuto conto delle loro caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.

CLAUSOLE TIPICHE DELLE CONDIZIONI GENERALI DI UTILIZZO DELL'APP

- **Contenuti e finalità dell'App per l'Utente**
- **Definizione Utenti**
- **Aggiornamenti**
- **Canone**
- **Recesso**
- **I Diritti di proprietà intellettuale sull'App**

2.2 Responsabilità civile per malfunzionamento dei dispositivi intelligenti

Provvedimenti dell'AGCM del 25 ottobre 2018 nei confronti di Apple e Samsung

L'AGCM ha accertato che Apple e Samsung hanno realizzato pratiche commerciali scorrette in violazione degli artt. 20, 21, 22 e 24 del Codice del Consumo in quanto hanno indotto i consumatori ad installare aggiornamenti su dispositivi non in grado di supportarli adeguatamente, senza fornire adeguate informazioni, causandone di fatto l'**OBSOLESCENZA PROGRAMMATA.**

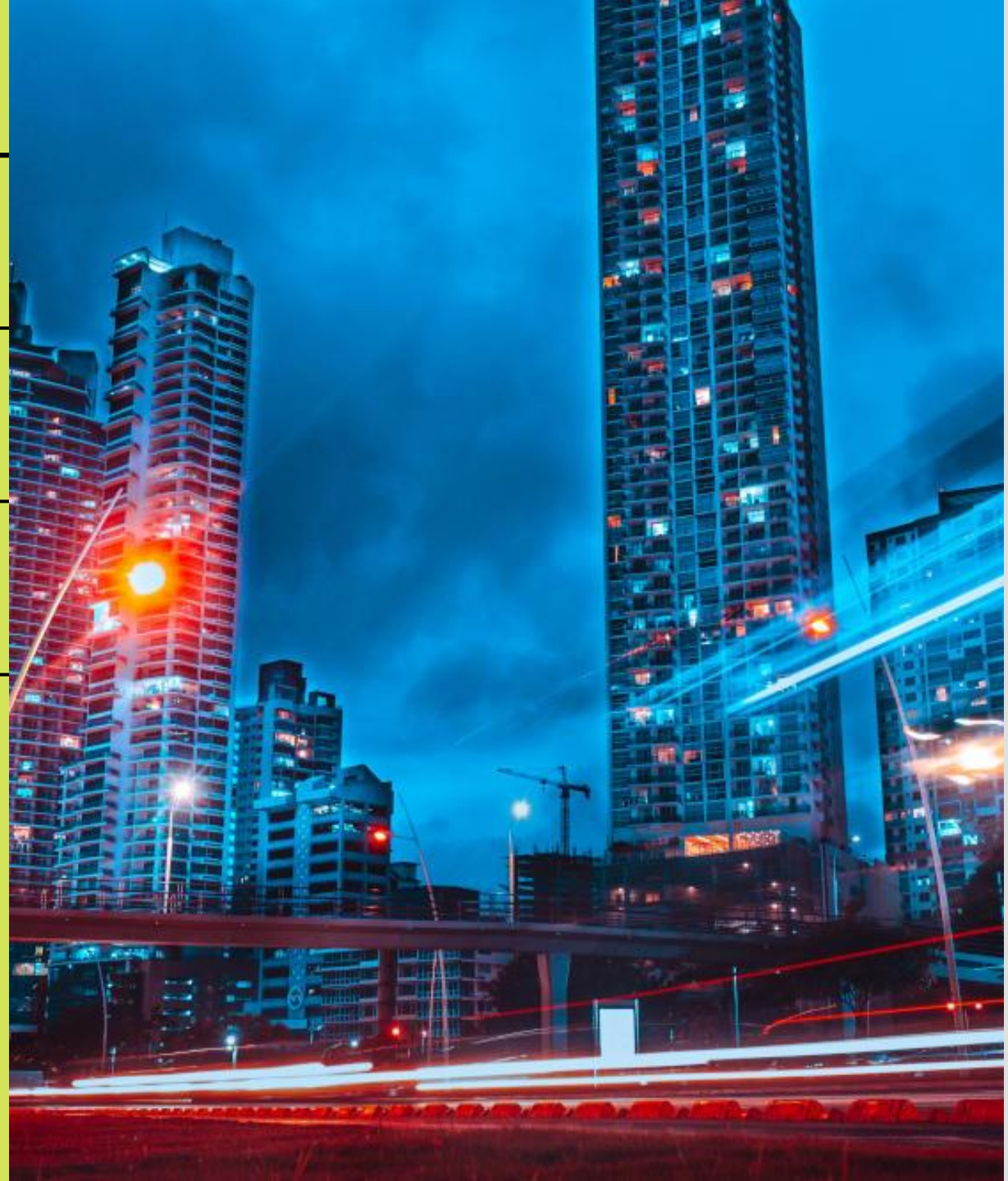
A Samsung e Apple sono state applicate sanzioni pari al **massimo edittale**: a Samsung 5 milioni di euro e ad Apple 10 milioni di euro (5 milioni per ciascuna delle due pratiche contestate).

2. PROBLEMATICHE GIURIDICHE DELL'IOT E DELL'IA

2.1 Trattamento e protezione dei dati personali dei trasmessi attraverso i dispostivi intelligenti

2.2 Assistenza post vendita e *remote customer care* digitalizzata: modelli contrattuali e clausole tipiche

2.3 **Responsabilità civile per malfunzionamento dei dispositivi intelligenti**



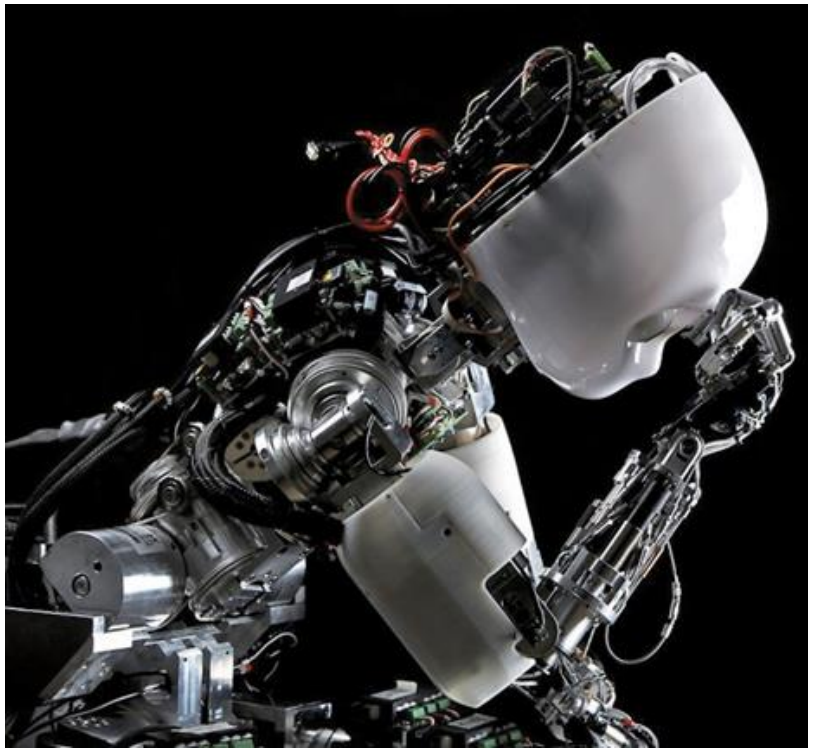
GLI OBBLIGHI GIURIDICI
A CARICO DELLE IMPRESE E I RELATIVI RISCHI

- L'**impresa**, se produttrice di dispostivi intelligenti, è **responsabile:**
  a. livello contrattuale, per difetti o difformità del prodotto, ai sensi del c.c. e del c.d.c.
  b. a livello extracontrattuale, per responsabilità del produttore ex art. 114, c.d.c., per i danni derivanti dai difetti di funzionamento del dispositivo qualora non offra la sicurezza che l'utente ragionevolmente può attendersi.

- I rischi a carico delle imprese variano a seconda che il dispositivo sia stato venduto nel mercato B2B e/o B2C.

- La disciplina consumeristica tipicamente prevede garanzie legali più lunghe e previsioni contrattualmente inderogabili.

2.3 Responsabilità civile per malfunzionamento dei dispositivi intelligenti



QUALE REGIME DI RESPONSABILITA' CIVILE PER L'IA?

FCA
FIAT CHRYSLER AUTOMOBILES

Nel 2015 grave vulnerabilità informatica che consentiva di prendere il controllo della vettura da remoto

2.3 Responsabilità civile per malfunzionamento dei dispositivi intelligenti

Responsabilità da Smart Product difettoso – Direttiva 85/374 CEE del 25 luglio 1985

- **Responsabilità del produttore** indipendentemente da colpa / dolo e dalla prevedibilità del danno
- Danneggiato deve **provare il difetto** del prodotto , il danno subito e il nesso di causalità
- Difetto «genetico»:
  - Vizi di fabbricazione che riguardano un solo esemplare;
  - Vizi di progettazione, che riguardano un'intera serie di prodotti

Quid iuris per l'Intelligenza artificiale?

2.3 Responsabilità civile per malfunzionamento dei dispositivi intelligenti

Opportuna interpretazione estensiva della nozione di difetto nel caso di smart product

Esempi:

- Mancata previsione di «blocchi di sicurezza» idonei ad impedire al prodotto intelligente di porre in essere determinate condotte;
- Mancata previsione di meccanismi volti a impedire l'esecuzione di comandi errati provenienti dall'uomo;
- Mancata previsione di barriere idonee a ostacolare aggressioni esterne e hackeraggi

Rilevanza dell'algoritmo di machine learning

Responsabilità del creatore dell'algoritmo quale produttore di una componente del prodotto finale

Attenuazione dell'onere della prova del difetto in capo al danneggiato

Corte di Giustizia UE, 5 marzo 2015, C – 503/13

«L'accertamento di un potenziale difetto di prodotti appartenenti alla medesima serie di produzione (nel caso di specie era un pacemaker)*, consente di qualificare come difettosi tutti i* ***prodotti di tale serie, senza che occorra dimostrare il difetto del prodotto interessato****» e «i costi per la loro sostituzione sono a carico delle aziende produttrici».*

Corte di Giustizia UE, 21 giugno 2017, C – 621/2015

Quando oggetto di contenzioso sono prodotti ad alta complessità tecnica e/o scientifica il danneggiato può avvalersi del metodo indiziario (indizi gravi, precisi e concordanti del difetto)

2.3 Responsabilità civile per malfunzionamento dei dispositivi intelligenti

Con la proposta di Risoluzione recante "*Raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica*", il Parlamento Europeo ha prospettato **due modelli di attribuzione della responsabilità** per IA:

- un regime di **responsabilità oggettiva o di "strict *liability*" del produttore**: in cui il produttore dello smart product è sempre responsabile per i danni cagionati dalla macchina, a prescindere da eventuali profili di dolo o di colpa;

- **un approccio di "gestione dei rischi",** per cui è responsabile chi, tra i soggetti potenzialmente coinvolti nella lesione, possa essere ritenuto responsabile del danno in quanto reputato "**causalmente più vicino al prodotto**".

Accanto a tale regime di responsabilità, il Parlamento Europeo ipotizza anche:

- l'**Istituzione di un regime assicurativo obbligatorio** relativo a categorie specifiche di robot *self-learning;*
- la **costituzione di un apposito fondo** per garantire al soggetto leso il risarcimento del danno cagionato dal robot;
- l'istituzione di una **forma di immatricolazione individuale dei robot**

2.3 Responsabilità civile per malfunzionamento dei dispositivi intelligenti

La prima decisione in tema di IA in Italia!

Consiglio di Stato, sez. IV, sentenza dell'8 aprile 2019

«*La decisione amministrativa automatizzata, impone al giudice di valutare la* ***correttezza del processo informatico*** *in tutte le sue componenti (costruzione, inserimento dei dati, validità e gestione degli stessi)*»

I giudici amministrativi incoraggiano l'ingresso nei procedimenti amministrativi delle nuove tecnologie informatiche, specie in quelli con procedure seriali standardizzabili, ma al tempo stesso sottolineano che ciò non può costituire motivo di elusione dei principi che regolano lo svolgersi dell'attività amministrativa.

CONTATTI

Avv. Eugenio Bettella

Managing Partner
Padova

T +39 049 8046911
eugenio.bettella@roedl.it

Avv. Giuliana Viviano

Associate Partner
Padova

T +39 049 8046911
giuliana.viviano@roedl.it

Avv. Margherita Cera

Associate
Padova

T +39 049 8046911
margherita.cera@roedl.it

CONTATTI

Rödl & Partner

Avvocati, Dottori Commercialisti, Revisori Legali e Consulenti del Lavoro
Attorneys-at-Law, Tax Consultants, Certified Public Accountants and Labour Consultancy
Rechtsanwälte, Steuerberater, Wirtschaftsprüfer, Arbeitsrechtsberater

Milano
Largo Donegani, 2
20121 (MI)
Tel.: +39-02-6328841
Fax: +39-02-63288420
info@roedl.it

Padova
Via F. Rismondo, 2/E
35131 (PD)
Tel.: +39-049-804 6911
Fax: +39-049-8046920
padua@roedl.it

Roma
P.zza S.Anastasia, 7
00186 (RM)
Tel.: +39-06-96701270
Fax: +39-06-3223394
roma@roedl.it

Bolzano
P.zza Walther- von- der- Vogelweide 8
39100 (BZ)
Tel.: +39-0471-1943200
Fax: +39-0471-1943220
bozen@roedl.it