

Febbraio 2019

Internet of Things e FinTech: evoluzione normativa di una rivoluzione tecnologica

Avv. Fabrizio Cascinelli e Avv. Cristina Bernasconi, PwC TLS Avvocati e Commercialisti

SOMMARIO: - 1. Introduzione: l'*Internet of Things* in breve; 2. L'*Internet of Things*: caratteristiche ed evoluzione normativa; 2.1. Definire un prodotto “smart” nell'*Internet of Things*; 2.2. Da un “*Internet of Things*” verso un “*Internet of People*”; 2.3. Soluzioni innovative di business a costo zero?; 2.4. La disciplina regolamentare dell'*Internet of Things*; 3. L'*Internet of Things* applicato; 3.1. Un mondo interconnesso: città, aziende, servizi; 3.2. Gli oggetti connessi nel *FinTech*; 4. Conclusioni.

1. Introduzione: l'Internet of Things in breve

Negli ultimi anni un'innovazione tecnologica di significativa importanza ha interessato i più svariati aspetti dell'economia, reale e finanziaria, gettando le basi per un miglioramento nel continuo dei processi produttivi e per la diffusione sempre più capillare di prodotti e sistemi integrati, volti a migliorare la cosiddetta esperienza d'uso di chi usufruisce di beni e servizi innovativi.

Tale progresso tecnologico è stato animato dalla volontà di costruire un mondo integrato, dove la realtà virtuale si potesse interfacciare ed integrare con il mondo reale, sulla base di un continuo flusso di scambio di dati che permettesse l'ottimizzazione dei servizi e la ricerca e lo sviluppo di soluzioni ancor più innovative.

È questo lo scenario nel quale si è sviluppato l'*Internet of Things* (anche “Internet delle cose” o, in breve, “IoT”), ovvero un ecosistema dove applicazioni e servizi funzionano grazie all'utilizzo di dati raccolti da strumenti connessi ed integrati al mondo “fisico”. Un fenomeno che ha contribuito ad apportare significativi cambiamenti nell'ambito dei più svariati settori dell'economia, dal mondo della salute, all'agricoltura, ai trasporti e al manifatturiero, nonché, in maniera particolare, nell'ambito dei servizi finanziari, creando una stretta connessione tra *Internet of Things* e *FinTech*.

Gli impatti generati da una simile evoluzione si sono verificati su larga scala, tanto da sollecitare l'attenzione dei Regolatori e rendere evidente la necessità di interventi volti a

disciplinare e armonizzare il fenomeno, così da guidarne gli sviluppi e l'implementazione in conformità con la normativa applicabile, con l'obiettivo primario della tutela dell'utilizzatore finale.

Dall'analisi del quadro normativo vigente emerge che gli sviluppi della materia hanno dato origine a sfide significative sotto il profilo regolamentare.

La disciplina dell'*Internet of Things* nel mercato dei servizi finanziari rimane ad oggi frammentata, sotto molteplici aspetti, nei diversi Stati membri, dal momento che i profili giuridici connessi sono regolati in maniera non uniforme: dalla tutela dei consumatori, alla disciplina di privacy e cyber security ai profili di responsabilità dei produttori e fornitori di servizi.

L'assenza di un *set* di regole armonizzato, pur non ostacolando la crescita e l'evoluzione del fenomeno *Internet of Things*, non agevola l'instaurazione di un mercato comune in cui alla base vi sia la tutela dell'utilizzatore finale. Ed è proprio sulla base dell'esigenza di instaurare un clima di fiducia tra i partecipanti al mercato che è emersa nel corso del tempo l'esigenza di armonizzare il panorama legislativo, pur nella consapevolezza delle difficoltà insite nel tentativo di definire con chiarezza e uniformità regole di un mondo in continua evoluzione.

2. L'Internet of Things: caratteristiche ed evoluzione normativa

Al fine di comprendere la portata del fenomeno, è opportuno effettuare un breve *excursus* dei concetti chiave e dell'evoluzione normativa che ha accompagnato lo sviluppo dell'*IoT*, con particolare riguardo al risvolto applicativo nell'ambito FinTech.

2.1. Definire un prodotto “smart” nell'Internet of Things

Ad oggi, i dati raccolti da strumenti connessi ed integrati al mondo “fisico” rendono possibile il funzionamento degli oggetti in modalità integrata e creano il background per lo sviluppo dell'*Internet of Things*.

Sebbene sia evidente ormai a tutti la portata di tale fenomeno, una definizione univoca di *Internet of Things* non è ancora stata coniata ufficialmente.

Il termine, coniato per la prima volta dal ricercatore del Massachusetts Institute of Technology Kevin Ashton nel 1999, è stato utilizzato secondo interpretazioni e adattamenti di volta in volta effettuati nei differenti contesti.

Nel 2011 l'Organizzazione per la cooperazione e lo sviluppo economico (in breve, “OECD”) ha utilizzato il termine *Internet of Things* con riferimento ai metodi di comunicazione e scambio dati c.d. “Machine to Machine” (“M2M”), riferendosi ad apparecchi e strumenti che comunicassero tra loro e che, nonostante non fossero

computer nel senso tradizionale, utilizzassero Internet¹. In tal modo, i dispositivi di *Internet of Things*, interconnessi tra loro grazie a un c.d. “approccio aperto”, utilizzano la connessione di rete per offrire servizi agli utenti e per interagire tra loro, creando un “ambiente smart”.

È su tale scorta che la Commissione Europea, nel 2012, si è riferita all'*Internet of Things* come quel “futuro in cui oggetti di uso quotidiano come telefoni, automobili, elettrodomestici, vestiti e persino alimenti sono collegati ad internet con una connessione senza fili tramite chip intelligenti e sono in grado di rilevare e comunicare dati”².

A prescindere dalle differenti definizioni che sono state coniate nel tempo, le caratteristiche chiave dell'*Internet of Things* possono dirsi univoche e ricorrenti: la quasi totale autonomia degli oggetti nonché il notevole scambio di dati tra gli oggetti stessi.

L'*Internet of Things* non richiede, infatti, ai fini del proprio funzionamento, un intervento umano preponderante e rende possibile uno scambio continuo di informazioni relative all'utilizzo degli oggetti, agli utilizzatori stessi e alle loro abitudini.

Le caratteristiche di tale fenomeno possono essere sintetizzate nelle seguenti³:

- (i) complessità, stante l'interazione dell'oggetto “smart” con l'ambiente circostante,
- (ii) autonomia, stante il minimo grado o la totale assenza di interazione umana ai fini del funzionamento dell'oggetto “smart”,

¹ Nell'ambito delle comunicazioni “M2M”, gli strumenti di *Internet of Things*, infatti, si collegano alla rete locale attraverso un indirizzo IP e, da questa fonte di accesso, raccolgono dati che a loro volta trasmettono a piattaforme *cloud*. In tal modo gli strumenti di *Internet of Things* rendono possibile l'accesso e la gestione dei dati da remoto, senza che sia necessaria una presenza fisica che interagisca con il dispositivo.

Si confronti, al riguardo, OECD (2012), *Machine-to-Machine Communications. Connecting billions of devices*, OECD Digital Economy Papers No. 192, reperibile sul sito istituzionale all'indirizzo: https://www.oecd-ilibrary.org/science-and-technology/machine-to-machine-communications_5k9gsh2gp043-en. In tale sede, l'OECD si è espresso nei seguenti termini: “(...) *Devices that are actively communicating using wired and wireless networks, that are not computers in the traditional sense and are using the Internet in some form or another. M2M communication is only one moment of smart meters, cities and lighting. It is when it is combined with the logic of cloud services, remote operation and interaction that these types of applications become “smart”.*”

² COMMISSIONE EUROPEA (2012), *Agenda digitale: la Commissione lancia una consultazione sulle regole per i dispositivi intelligenti connessi – l'“internet delle cose”.*

³ COMMISSIONE EUROPEA (2018), *Liability for emerging digital technologies. Commission Staff Working Document accompanying the document “Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions”, Commission Staff Working Document, Brussels, 25 April 2018, SWD(2018)137final.*

- (iii) focalizzazione sui dati, stante lo scambio di dati in quantità significative,
- (iv) architettura aperta, che incorpora elementi tangibili e intangibili.

La circostanza che l'interazione tra il mondo fisico e il mondo digitale, attraverso flussi continui di dati, rende disponibile una quantità significativa di informazioni concernenti i dispositivi utilizzati e i relativi utenti finali rende centrale il relativo patrimonio informativo. È del tutto evidente che, in un contesto dove l'interazione umana è richiesta in misura minore, la figura dell'utente finale acquisisca in ogni caso una significativa importanza agli occhi dei fornitori e gestori degli oggetti connessi, in quanto fonte di una mole di dati importante.

È in questo modo che l'*Internet of Things* può diventare un "*Internet of People*"⁴, focalizzato sulla quantità significativa di informazioni che possono essere raccolte.

2.2. Da un "*Internet of Things*" verso un "*Internet of People*"

L'*Internet of Things*, proiettato verso una dimensione "*Internet of People*" focalizzata sulla figura dell'utente che usufruisce dei dispositivi connessi, funziona e si sviluppa grazie al supporto di ulteriori sistemi e applicativi che rendono possibile l'effettivo scambio di dati e informazioni: spazi di archiviazione, regole e dispositivi di gestione di un quantitativo ingente di dati.

L'*Internet of Things* si inserisce, infatti, nel contesto della gestione dei *Big Data*, ovvero nell'utilizzo di sistemi IT altamente sviluppati, finalizzati alla gestione e al processamento di un numero significativo di dati, anche di differenti tipologie. Tale mole significativa di informazioni può senza dubbio agevolare la creazione di prodotti e servizi personalizzati sulla base delle esigenze degli utilizzatori, i cui dati sono scambiati tramite i relativi oggetti connessi. Dati che sono raccolti attraverso piattaforme *cloud* che ne permettono l'archiviazione.

Proprio la combinazione tra *Internet of Things*, *Cloud computing* e *Big Data* dovrebbero contribuire alla creazione di c.d. "*smart environments*" dove ulteriori e innovativi servizi potranno essere sviluppati grazie alla significativa mole di dati scambiati. A tal fine, non potranno che giovare le creazioni di piattaforme orizzontali di scambio di dati che permettano l'interazione tra gli operatori del settore e la realizzazione di economie di scala⁵.

⁴ VIVIANE REDING (2006), *RFID: Why we need a European policy*, EU RFID 2006 Conference: heading for the Future, Brussels, 16 October 2006, SPEECH/06/597. Viviane Reding talked at EU RFID 2006 Conference as a member of the European Commission responsible for the Information Society and Media.

⁵ COMMISSIONE EUROPEA (2013), *Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination. Final Report. A study prepared for the European Commission*, DG Communications Networks, Content & Technology, 2013/0037.

In tale contesto, diviene fondamentale comprendere come gestire tali dati, nel rispetto della privacy degli utenti, assicurando la sicurezza dei flussi informativi e delle modalità di raccolta e garantendo il minor impatto possibile dei potenziali rischi che la diffusione su larga scala dell'*Internet of Things* può comportare.

È pur vero che la creazione di un ambiente integrato e caratterizzato dall'interoperabilità degli oggetti connessi può esistere solo laddove tutti i soggetti coinvolti siano in grado di sostenere i costi di un simile cambiamento. Al riguardo, è evidente come un freno allo sviluppo di tali fattispecie potrebbe essere costituito dalla difficoltà per piccole e medie imprese nell'adottare soluzioni tecnologiche innovative su larga scala al fine di interagire con il fenomeno dell'*Internet of Things*.

2.3. Soluzioni innovative di business a costo zero?

Lo sviluppo dell'*Internet of Things* è stato dettato anche dai molteplici benefici che esso comporta per gli utenti finali, configurando un valido supporto per lo svolgimento delle attività e lo sviluppo di soluzioni innovative di business.

In primo luogo, un mondo interconnesso caratterizzato da dispositivi “smart”, capaci di raccogliere e trasmettere dati, rappresenta l'occasione per personalizzare beni e servizi, a beneficio della c.d. “*customer experience*”. La personalizzazione di beni e servizi è resa possibile anche grazie all'utilizzo del c.d. Big Data che, generando un flusso di dati significativo, permette di raccogliere informazioni, preferenze e caratteristiche degli utilizzatori degli oggetti connessi.

A tal riguardo, con particolare riferimento al settore dei servizi bancari finanziari e assicurativi, è stato osservato dalle Autorità di Vigilanza di settore come i flussi informativi, relativi agli utenti e all'utilizzo da parte di questi ultimi degli oggetti, possano effettivamente rappresentare un punto di svolta nell'ambito dei processi produttivi⁶. Essi permettono di identificare le caratteristiche chiave degli utenti finali e di creare, di conseguenza, prodotti “customizzati” e di offrirli alle categorie di clienti per le quali sono stati ideati.

I dati raccolti potrebbero essere utilizzati, infatti, a scopi di profilatura della clientela, monitoraggio del gradimento del prodotto da parte dei clienti, valutazioni del merito creditizio, campagne di marketing, sviluppo dei prodotti, test di adeguatezza/appropriatezza, test sui bisogni e esigenze dei clienti, definizione del *pricing* dei prodotti, sviluppo dei controlli a fini antiriciclaggio, supporto nella valutazione dei processi distributivi⁷.

⁶ ESAs (2016), *Joint Committee Discussion Paper on the Use of Big Data by Financial Institutions*, JC 2016 86.

⁷ ESAs (2016), *Joint Committee Discussion Paper on the Use of Big Data by Financial Institutions*, JC 2016 86.

In secondo luogo, una diffusione sempre più capillare di conoscenze è il punto di partenza per pensare e costruire i prodotti destinati a soddisfare le esigenze degli utenti secondo nuove modalità, usufruendo dei flussi continui di dati e rendendo possibile l'inclusione degli utenti in determinati segmenti di clientela, così da razionalizzare il mercato. Nel contesto dell'*Internet of Things*, infatti, è sorta e si è sviluppata la c.d. “*Next Production Revolution*” (NPR), basata su un know-how di conoscenza acquisito tramite flussi continui di dati e caratterizzata, peraltro, su un funzionamento quasi autonomo delle macchine nell'ambito dei processi produttivi, dove l'intervento umano sarebbe stato richiesto solo in sede di controllo⁸.

I benefici apportati dall'*Internet of Things*, tuttavia, non sono privi di profili critici che rischiano di inficiare l'efficienza del fenomeno e di rallentare la diffusione sempre più capillare.

La disponibilità di una quantità significativa di dati relativi agli utilizzatori e alle relative abitudini di consumo potrebbe indurre i detentori di tali informazioni (*i.e.* le istituzioni creditizie, imprese di assicurazione e gli altri soggetti regolati, se pensiamo al mondo dei servizi finanziari) a proporre offerte sempre più targettizzate al cliente, senza dare a quest'ultimo la possibilità di comparare i prodotti e comprendere effettivamente l'opportunità di effettuare tale scelta. Con particolare riferimento alla categoria dei rischi, ciò potrebbe indurre banche e imprese di assicurazione a modificare i profili di rischio dei clienti, rispettivamente per il rischio di credito e l'apprezzamento del rischio da assicurare, sulla base delle informazioni raccolte senza interagire realmente con il cliente, bensì grazie al monitoraggio di abitudini di consumo o di eventi, delle cui informazioni gli oggetti connessi tengono traccia⁹. Un primo esempio applicativo nel settore dei servizi assicurativi si è avuto con l'introduzione delle c.d. “scatole nere” (“*telematic boxes*”), installate nelle automobili e capaci di monitorare il comportamento degli utenti alla guida, ed utilizzate quali fonti di dati per costruire e offrire prodotti assicurativi più aderenti, anche in termini di tariffa, al profilo di rischio dell'assicurato. Allo stesso modo, sempre nel settore assicurativo, sono stati introdotte le c.d. “*smart home*” che attraverso la raccolta di dati trasmessi da oggetti connessi possono contribuire a costruire polizze personalizzate a protezione della casa.

È evidente come in tale ambito sussista un rischio che l'utilizzatore finale di questi servizi possa perdere il controllo sui propri dati raccolti e sull'utilizzo che i soggetti detentori di tali dati potrebbero farne.

Il rischio di un utilizzo scorretto dei dati, oltre a minare la fiducia degli utenti, potrebbe generare conseguenze negative per gli operatori del settore: le istituzioni finanziarie

⁸ OECD (2016), *The Internet of Things. Seizing the benefits and addressing the challenges. 2016 Ministerial Meeting on the Digital Economy. Background report*, OECD Digital Economy Papers No. 252, pag. 12 ss.

⁹ ESAs (2016), *Joint Committee Discussion Paper on the Use of Big Data by Financial Institutions*, JC 2016 86.

stesse potrebbero rispondere di danni reputazionali e patrimoniali non indifferenti, laddove sia effettivamente provato un utilizzo non conforme dei dati degli utenti.

Ad alimentare potenzialmente tali preoccupazioni, vi è anche il rischio che, a fronte di un continuo flusso di dati, i dati stessi siano trasmessi o recepiti in maniera fuorviante dagli oggetti “smart”. In tal modo vi sarebbe il rischio di una lettura dei dati potenzialmente fuorviante che genererebbe una analisi scorretta degli stessi¹⁰.

Alla luce di tali aspetti, è emersa da più parti l’esigenza di definire un quadro regolamentare più puntuale che potesse fornire una linea guida per gli operatori del settore e maggiore sicurezza per gli utenti, garantendo la raccolta e l’utilizzo dei dati con pratiche non aggressive e l’impostazione di controlli automatizzati che possano identificare eventuali errori¹¹.

2.4. La disciplina regolamentare dell’Internet of Things

Un mondo in continua evoluzione come quello dell’*Internet of Things* poco si concilia con le tempistiche e le esigenze sottese all’adozione di nuove norme. Non è infatti un caso se la disciplina regolamentare di tale fenomeno sia lacunosa o, perlomeno a livello europeo, frammentata nei diversi Stati Membri, dove le differenti tematiche sono affrontate e gestite in modalità differenti.

La mancanza di un quadro normativo completo e unitario, tuttavia, comporta non poche difficoltà: prima fra tutte, la discontinuità e l’eventualità che possano esservi delle criticità nello scambio transfrontaliero di dati, la disomogeneità di raccolta e archiviazione dei dati e, non ultimo, il rischio di una capillare diffusione di una generale mancanza di fiducia tra i partecipanti al mercato rispetto all’utilizzo degli oggetti connessi in assenza di regole certe¹².

Un panorama frammentato come quello dell’*Internet of Things* necessita di un quadro regolamentare che ne armonizzi la disciplina e riesca a gestire in modo omogeneo gli eventuali rischi che potrebbero inficiare l’efficienza del funzionamento di dispositivi di *Internet of Things*, ai danni dell’utente finale.

¹⁰ La portata degli impatti di una simile circostanza, evidentemente, potrebbe variare in considerazione dell’ambito di riferimento: sarebbe particolarmente elevata, a titolo esemplificativo, nel settore della ricerca medica. A tal riguardo, si confronti OECD (2016), *The Internet of Things. Seizing the benefits and addressing the challenges. 2016 Ministerial Meeting on the Digital Economy. Background report*, OECD Digital Economy Papers No. 252.

¹¹ A tal riguardo si confronti BASEL COMMITTEE ON BANKING SUPERVISION, *Implications of fintech developments for banks and bank supervisors*, February 2018. Si confronti altresì COMMISSIONE EUROPEA (2017), *Big Data: a complex and evolving regulatory framework, Digital Transformation Monitor*, January 2017. Al riguardo, infine, OECD (2016), *The Internet of Things. Seizing the benefits and addressing the challenges. 2016 Ministerial Meeting on the Digital Economy. Background report*, OECD Digital Economy Papers No. 252.

¹² COMMISSIONE EUROPEA (2017), *Big Data: a complex and evolving regulatory framework, Digital Transformation Monitor*, January 2017.

Nonostante tali difficoltà, il Regolatore europeo ha cercato di porvi rimedio e gettare le basi per una armonizzazione legislativa dei temi più sensibili, che potessero far fronte alle evoluzioni sorte con il diffondersi e il progredire dell'*Internet of Things*.

Gli albori dell'Internet of Things nel panorama legislativo

Nel 2006 la Commissione Europea ha avviato una pubblica consultazione destinata a comprendere le esigenze normative e il quadro regolamentare più idoneo relativo alla produzione e all'utilizzo di "smart chips" fondati su tecnologia di identificazione a radiofrequenza (c.d. "RFID"). Tali dispositivi, che all'epoca si stavano diffondendo al fine di sostituire i codici a barre tradizionali, avrebbero ampliato le possibilità di localizzazione, identificazione e tracciabilità dei dati, ma al tempo stesso avrebbero potenzialmente ampliato i rischi di violazione della privacy nonché ridotto la sicurezza dei dati stessi.

L'interesse del Regolatore europeo, pertanto, era volto ad assicurare che tale innovazione tecnologica potesse diffondersi, senza rappresentare alcun danno per gli utenti finali, e aprire la strada a un progresso tecnologico sempre più capillare, caratterizzato da oggetti interconnessi "in un internet delle cose" che avrebbe permesso di "migliorare notevolmente il benessere economico e la qualità della vita"¹³. Ciò sarebbe stato possibile solo definendo, a livello armonizzato, la disciplina normativa delle prassi in materia, nel rispetto della riservatezza dei dati e dei principi etici nella tecnologia¹⁴.

Gli esiti della consultazione, pubblicati nel 2007 hanno messo in luce lo scetticismo del mercato in relazione alla diffusione di una tecnologia interconnessa e al necessario scambio di dati che ne sarebbe conseguito, senza che vi fossero certezze in merito ai controlli e presidi posti in essere¹⁵. A fronte della necessità di superare il gap informativo in materia e diffondere la consapevolezza che il progresso tecnologico fosse un fenomeno regolamentato, la Commissione europea ha pubblicato la pianificazione di azioni che avrebbe attivato, al fine di elaborare la strategia più idonea in materia di RFID. In particolare, sarebbe stato istituito un "gruppo" ad hoc in grado di assistere la Commissione europea in materia; sarebbe stata oggetto di riesame e aggiornamento la normativa comunitaria relativa alle telecomunicazioni e alle comunicazioni elettroniche, nonché la disciplina della sicurezza dei dati e della tutela della privacy, al fine di creare il corretto inquadramento normativo del progresso tecnologico¹⁶.

¹³ COMMISSIONE EUROPEA (2006), *La Commissione avvia una consultazione pubblica sulle etichette che utilizzano dispositivi di identificazione a radiofrequenza*, Bruxelles, 8 marzo 2006, IP/06/289.

¹⁴ COMMISSIONE EUROPEA (2006), *Commission opens online public consultation on radio frequency identification (RFID)*, Bruxelles, 3 luglio 2006, IP/06/909.

¹⁵ COMMISSIONE EUROPEA (2007), *La Commissione propone una strategia europea per le etichette intelligenti a radiofrequenza*, Bruxelles, Hannover, 15 marzo 2007, IP/07/332.

¹⁶ COMMISSIONE EUROPEA (2006), *Radio Frequency Identification Devices (RFID): Frequently Asked Questions*, Bruxelles, 9 marzo 2006, MEMO/06/112.

I piani di sviluppo della regolamentazione dell'Internet of Things

Nel corso del triennio 2006-2009 il progresso tecnologico ha conosciuto uno sviluppo notevole: le applicazioni che collegano oggetti a *internet* e fra di loro stessi sono proliferate in maniera significativa per numero e tipologia. Numerosi ne sono stati gli esempi, come ricordato dalla allora Commissaria europea per la Società dell'informazione e i media: auto collegate ai semafori, elettrodomestici collegati a reti elettriche intelligenti, misuratori di energia elettrica per monitorare e ridurre i consumi. A fronte di tale incremento e della sempre più attuale esigenza di regolare in maniera uniforme il fenomeno, tenendone presidiati le potenziali criticità, la Commissione Europea nel 2009 ha individuato quattordici azioni “*intese a promuovere lo sviluppo dell'internet degli oggetti*”¹⁷.

Se nel 2006 il primo pensiero del Regolatore era stato volto alla disciplina della tecnologia RFID, ora il fenomeno si stava sviluppando ad una tale portata da richiedere un intervento a più ampio spettro.

In tale contesto, la Commissione Europea nel proprio *action plan* del 2009 individua quattordici ambiti di intervento¹⁸: (i) costruzione di un assetto di *governance* per la gestione dell'*Internet of Things*; (ii) gestione degli impatti rispetto alla disciplina di *privacy* e sicurezza dei dati; (iii) necessità di garantire agli utenti il c.d. “diritto al silenzio dei dispositivi”, permettendo loro di eliminare i dati condivisi e disconnettersi dagli oggetti collegati a *Internet* in ogni momento; (iv) predisposizione di azioni idonee a garantire sicurezza e *privacy* dei dati; (v) sviluppo di *Internet of Things* quale risorsa essenziale per la crescita dell'Europa; (vi) definizione di linee guida standard al fine di uniformare la disciplina di *Internet of Things*; (vii) finanziamento della ricerca; (viii) sviluppo delle c.d. “*Public Private Partnership*” al fine di incrementare l'*Internet of Things*; (ix) diffusione di progetti pilota per assicurare il grado di innovazione più alto possibile; (x) avvio di tavoli di lavoro con le istituzioni europee (Parlamento Europeo e Consiglio); (xi) condivisione di informazioni e piani strategici di sviluppo con i partner internazionali; (xii) impatto ambientale del riciclo delle tecnologie RFID; (xiii) analisi di mercato relative agli utilizzi delle tecnologie RFID; (xiv) monitoraggio della evoluzione normativa dell'*Internet of Things*.

Alla luce delle potenziali criticità dell'*Internet of Things* e della vasta portata degli interventi che lo sviluppo delle 14 linee d'azione avrebbe richiesto, la Commissione Europea ha proseguito nella definizione del background regolamentare il più possibile aderente ai principi dell'Unione Europea e, nel 2012, ha avviato una ulteriore

¹⁷ COMMISSIONE EUROPEA (2009), *Quando i vasetti dello yogurt cominciano a parlarvi: l'Europa si prepara alla rivoluzione di internet*, Bruxelles, 18 giugno 2009, IP/09/952.

¹⁸ La Commissione Europea, nell'ambito della Comunicazione IP/09/952 ha previsto in allegato “*14-point action plan*” che include: “*governance, privacy and data protection, the right to the “silence of the chips”, emerging risks, vital resource, standardisation, research, public private partnership, innovation, institutional awareness, international dialogue, environment, statistics, evolution*”.

consultazione sulle regole per i dispositivi intelligenti connessi. Tale intervento era volto a identificare le misure più idonee per garantire il prosieguo dell'innovazione tecnologica nel rispetto dei diritti degli utenti finali, ed in particolare del diritto alla riservatezza di informazioni quali i modelli comportamentali, ubicazione e preferenze degli utenti stessi.

Verso un mercato digitale unico

I passaggi normativi si sono susseguiti velocemente nel tempo. Nel marzo 2015 la Commissione Europea ha attivato il programma *Alliance for Internet of Things Innovation* (AIOTI) al fine di supportare la creazione di una “*industry 4.0*” armonizzata a livello europeo. Costituita nel settembre 2016 grazie al supporto di alcuni players del settore¹⁹, AIOTI è una organizzazione no-profit che ha l'intento di costruire un network a livello europeo per lo sviluppo dell'*Internet of Things*, dando la possibilità alle industrie del settore di condividere spunti di riflessione e know-how in tale ambito.

Tale iniziativa è stata avviata ed implementata di pari passo con la creazione di un mercato unico europeo del digitale: il “*Digital Single Market*” (DSM).

Instaurato nel 2015, il “*Digital Single Market*” si affianca agli altri tentativi del regolatore europeo di creare realtà uniche ed armonizzate nei settori che più di altri necessitano di cardini e principi comuni che ne definiscano con chiarezza l'assetto e che rendano concreta la possibilità di una commercializzazione di prodotti e servizi transfrontaliera.

Tale necessità di interazione e abbattimento delle “frontiere legislative” è percepita con particolare cura e attenzione in un ambito come quello del digitale dove l'interoperabilità diventa un elemento essenziale ai fini del buon funzionamento del sistema.

È sullo sfondo di tale quadro regolamentare che l'*Internet of Things* è stato sviluppato in Europa: esso non può che trarre beneficio da un sistema interconnesso e da una regolamentazione unitaria, guidata in ciascun Stato Membro dell'Unione Europea da principi fondamentali comuni.

L'esigenza di costruire un mercato unico dell'*Internet of Things* può dirsi uno dei pilastri che hanno caratterizzato lo sviluppo di una industria europea del digitale: un mondo nel quale esistano effettivamente oggetti connessi, che possano essere identificati in modo sicuro e che possano coesistere “integrati”, nonostante i volumi di dati scambiati.

¹⁹ Tra questi si ricordano: ARTEMISIA, Arthur's Legal, ATOS, Bosch, BT, CNH Industrial, Digital Catapult, Engineering LOI, GRADIANT, Huawei, IBM, Infineon Technologies, John Deere, Nokia, Philips Lighting, Samsung, Schneider Electric, Siemens, STMicroelectronics, Telit Communications, and Vodafone (secondo i dati risultanti dal sito istituzionale).

Proprio per l'esigenza di gestire una tale mole di dati, nel 2017 è stata avviata l'iniziativa europea c.d. "European data economy", volta a identificare le soluzioni più idonee e le scelte legislative più opportune per regolare lo scambio di dati su base transfrontaliera e disciplinare alcuni degli aspetti giuridici più sensibili su cui l'*Internet of Things* ha un impatto significativo. Tra questi, il regime di responsabilità collegato agli oggetti interconnessi – alla cui produzione e funzionamento contribuiscono soggetti giuridici differenti – i presidi privacy, gestione dei rischi.

I prossimi passi

L'esigenza di creare un framework normativo stabile e armonizzato a livello europeo è stata riconosciuta, nuovamente nell'aprile 2018, anche dalla Commissione Europea stessa, che al riguardo ha evidenziato la correlazione tra l'esistenza di tale set definito di regole e lo sviluppo degli investimenti nel settore delle tecnologie digitali innovative²⁰. In particolare, la Commissione Europea ha sollecitato la definizione di regole chiare in materia di responsabilità in caso di evento dannoso a carico degli utenti di oggetti connessi, al fine di armonizzare a livello europeo il regime di responsabilità contrattuale ed extra-contrattuale con riferimento alla fornitura di prodotti e servizi.

Alla luce di tali esigenze di chiarezza e uniformità, nel 2018 la Commissione Europea ha ribadito la necessità di un intervento normativo in materia, proponendo una serie di interventi volti a presidiare gli aspetti chiave, ai fini di una più efficiente evoluzione delle modalità di approccio al mercato, nel pieno rispetto dei principi chiave dell'Unione Europea. A tal proposito, la Commissione Europea ha pubblicato un "FinTech Action plan"²¹, nel quale ha appositamente previsto di prendere in carico la regolamentazione dei principali temi in materia (e.g. *cloud computing, distributed ledger technologies*) al fine di fornire un supporto concreto allo sviluppo delle innovazioni tecnologiche nel mondo del *FinTech*.

²⁰ La Commissione Europea ha dichiarato: "(...) *In order to fully benefit from the opportunities presented by these new products and services, stimulating investment in emerging digital technologies is critical. A clear and stable legal framework will stimulate investment and, in combination with research and innovation, will help bring the benefits of these technologies to every business and citizen*". Al riguardo si confronti COMMISSIONE EUROPEA (2018), *Liability for emerging digital technologies, Commission Staff Working Document accompanying the document "Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions"*, Commission Staff Working Document, Brussels, 25 April 2018, SWD(2018)137final.

²¹ COMMISSIONE EUROPEA (2018), *FinTech Action plan: For a more competitive and innovative European financial sector, Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions*, Brussels, COM(2018)109/2.

3. L'Internet of Things applicato

3.1. Un mondo interconnesso: città, aziende, servizi

Evidenti i benefici che lo scambio continuo di dati può comportare, l'*Internet of Things* si è ben presto diffuso nei più svariati campi della ricerca e nei vari settori dell'economia.

Esistono settori economici che ormai da lungo tempo conoscono l'*Internet of Things* e ne sfruttano i relativi benefici: si pensi alla videosorveglianza e alla sicurezza, al monitoraggio dei consumi "domestici" e alla mobilità dove esistono dispositivi quali i c.d. "semafori intelligenti" che dovrebbero agevolare il controllo del traffico, gli applicativi di "smart home" (e.g. televisori, frigoriferi) e "smart metering" per la registrazione di determinati parametri. Uno dei primi e forse più ricettivi settori dove l'*Internet of Things* si è sviluppato è il settore automotive, nell'ambito del quale sono sorte le c.d. "connected cars"²².

Tali dispositivi "intelligenti" sono stati ideati e costruiti senz'altro nell'ottica di agevolare l'utente finale, creando un mondo interconnesso che apportasse concreti benefici nelle esigenze quotidiane.

Ugualmente, importanti progressi sono avvenuti nel mondo dell'industria, con il tentativo di accelerare e automatizzare in maniera massiva i relativi processi di produzione, prevedendo apposite soluzioni digitalizzate.

È con queste finalità che si è andato creando un connubio significativo tra l'*Internet of Things* e la c.d. "Industry 4.0", cercando di consolidare l'introduzione della robotica e delle innovazioni digitali nel mondo dell'industria dando vita a uno "smart manufacturing". Alcuni settori hanno captato prima di altri le opportunità di sviluppo di un mondo interconnesso, dove fosse possibile una integrazione a livello verticale e orizzontale. Ciò significa che nell'ambito di un medesimo processo produttivo, gli oggetti "intelligenti" avrebbero permesso lo scambio di dati al fine di agevolare la produzione e monitorare ogni passaggio della stessa. Ugualmente, lo scambio capillare di dati e informazioni, tramite Internet, avrebbe reso possibile integrare differenti processi e avrebbe reso possibile il monitoraggio della *customer experience* in tempi utili per modificare, se del caso, la produzione di beni o servizi.

Vi sono, altresì, settori nell'ambito dei quali gli applicativi di "Internet of Things" possono dirsi ancora sperimentali, dal momento che le innovazioni progrediscono senza quella velocità che è ormai usuale in altri ambiti: il campo medico della c.d. "eHealth", che risente della necessità di ottenere significativi contributi pubblici.

Sebbene i tempi di sviluppo e progressione delle innovazioni non siano tempestivi, il settore della salute senz'altro ha beneficiato e potrà continuare a beneficiare di

²² EUROPEAN COMMISSION (2015), *Internet of Things: Connected cars*, Case Study 43.

dispositivi interconnessi capaci di trasmettere una quantità di dati significativa in forma anonima che agevoli la ricerca.

Lo sviluppo e il diffondersi dell'*Internet of Things* nell'ambito dei differenti settori economici ha con tutta evidenza rivoluzionato il mercato e le modalità di approcciarsi ai canali di business. La creazione di oggetti interconnessi rende evidente l'esigenza di integrare i canali e le competenze produttive: la categorizzazione di ciascun settore produttivo, attraverso l'individuazione di specifici target di mercato per ciascuno di essi, permette di costruire un prodotto e servizio a valore aggiunto in favore del cliente.

Tale segmentazione del mercato può avvenire su base verticale e su base orizzontale, focalizzandosi sullo sviluppo di un settore in particolare o, alternativamente, sullo sviluppo di relazioni commerciali al di fuori di settori che usualmente non erano raggiungibili in assenza di logiche di sviluppo tecnologico.

In tal modo, le imprese hanno potuto sviluppare aree di business differenti rispetto al core business: imprese produttive che hanno spostato il proprio asse di interesse verso prodotti a valore aggiunto, associati a servizi che possano offrire al cliente una *customer experience* migliore, e, viceversa, *softwarehouse* e imprese di servizi che hanno lanciato sul mercato oggetti connessi rientranti a pieno titolo nel mondo dell'*Internet of Things* (ad esempio lo strumento di "smart home" di Amazon e il Pixel smartphone di Google)²³.

3.2. Gli oggetti connessi nel FinTech

L'*Internet of Things* si sta imponendo anche nell'ambito del settore finanziario, rivoluzionando i modelli di business che lo caratterizzano. Il settore dei soggetti vigilati (*i.e.* settore bancario, finanziario e assicurativo) è uno di quei settori che più di altri hanno subito negli ultimi anni l'impatto dell'innovazione tecnologica, ma che al tempo stesso hanno risentito della staticità dei propri meccanismi e processi. A differenza di settori che nascono nell'ambito dell'innovazione e della tecnologia, il settore regolamentato è costretto a un costante e massivo aggiornamento, al fine di permettere alle strutture aziendali di stare al passo con lo sviluppo tecnologico sempre più capillare e in conformità con la normativa di riferimento, che lentamente si adegua e recepisce le innovazioni²⁴.

È su questo sfondo di contrasti tra esigenze di innovazione e necessità di mantenere saldi i principi di tutela della clientela e fiducia dei mercati che si è sviluppato l'*Internet of Things* nel settore del *FinTech*, dove il mondo tecnologico ha incontrato quello regolamentato dei soggetti vigilati.

²³ PWC (2017), *Cross-Cutting Business Models for IoT, Final Report, A study prepared for the European Commission, DG Communications Networks, Content & Technology, 2016/0027.*

²⁴ EBA (2018), *EBA Report on the impact of FinTech on incumbent credit institutions' business models*, 03 July 2018.

L'esigenza di un profondo rinnovamento di processi e modelli di business degli istituti creditizi e finanziari è sorta, a fronte di nuovi strumenti tecnologici disponibili sul mercato, al fine di garantire una maggiore velocità e funzionalità di accesso ai servizi, pur mantenendo alto il livello di sicurezza e integra la fiducia dei clienti, nonché al fine di non perdere quote di mercato²⁵.

Oggi, infatti, stanno crescendo le possibilità di accesso al mercato dei servizi finanziari per soggetti che possono vantare competenze tecnologiche specifiche: le c.d. *BigTech Companies*²⁶. Queste ultime, infatti, nei limiti in cui i servizi prestati non rientrano nell'ambito di specifiche riserve di attività, potrebbero essere in grado di offrire servizi e prodotti sfruttando i propri know-how altamente specializzati e presentarsi come concorrenti di soggetti regolamentati nell'ambito del rapporto cliente-fornitore di servizi.

Al tempo stesso, le *BigTech Companies* conoscono per la prima volta la necessità di inquadarsi in un mondo di regole che si sta definendo e che richiede il più delle volte specifiche autorizzazioni ai fini dell'operatività. Le stesse potrebbero considerare l'eventualità di espandersi nel settore regolamentato e, alla presenza di determinate condizioni, richiedere le dovute autorizzazioni alle Autorità di Vigilanza al fine di operare sui mercati.

L'integrazione dello sviluppo tecnologico nel mondo regolamentato dei servizi bancari, finanziari e assicurativi, tuttavia, non presenta esclusivamente ostacoli nella propria realizzazione. Anzi, una vasta gamma di opportunità può presentarsi per tutti i soggetti coinvolti: nuove potenziali partnership commerciali possono sorgere e nuovi potenziali sviluppi di modelli produttivi si stanno implementando, dove ciascuno dei soggetti coinvolti apporterebbe le proprie competenze e risorse al fine di creare una soluzione efficiente.

Tale integrazione, peraltro, potrebbe essere sempre più capillare in una dimensione come quella dell'*Internet of Things* dove i prodotti sono di per sé connessi e dove ciascun fornitore di prodotti e servizi è portatore di uno specifico know-how.

La diffusione dell'*Internet of Things* nell'ambito del *FinTech*, che oggi sta cominciando ad affermarsi in alcuni settori specifici, è stata peraltro anticipata da un impatto tecnologico verificatosi in particolare in alcuni settori del mondo bancario.

Tra questi, senz'altro ha subito forti cambiamenti il settore dei servizi di pagamento, dove già da tempo si stanno implementando strumenti e tecnologie che richiedono l'interazione con l'utente e che rendono possibile la trasmissione in tempo reale di

²⁵ CONSOB (2018), *Inaugurazione del Corso di Alta Formazione Fintech e Diritto*, ABI, Intervento di Paolo Ciocca, Commissario CONSOB, Roma, 10 maggio 2018.

²⁶ PANETTA (2018), *Fintech and banking: today and tomorrow. Speech by the Deputy Governor of the Bank of Italy Fabio Panetta*, Harvard Law School Bicentennial, Annual Reunion of the Harvard Law School Association of Europe, Rome, 12 May 2018.

quantità significative di dati. A tal proposito stiamo assistendo all'implementazione di nuove misure di autenticazione dell'identità del soggetto che dispone un'operazione di pagamento, anche attraverso dispositivi che raccolgono e trasmettono in tempo reale dati biometrici, identificano e verificano le generalità della clientela estrapolate da fotografie di documenti di identità, validandone le credenziali di autenticazione²⁷. Tale sviluppo tecnologico non è avvenuto senza un debito inquadramento normativo, stabilito dal Legislatore europeo e completato a livello nazionale (e.g. si pensi al riguardo alla Direttiva PSD2 in corso di implementazione negli Stati membri dell'UE).

Anche nell'ambito della normativa antiriciclaggio, con particolare riferimento alle modalità di adempimento dell'adeguata verifica²⁸, si è recentemente assistito a una accelerazione nell'utilizzo di tecnologie innovative che attingono anche al mondo dell'IoT.

Come noto, i soggetti obbligati agli adempimenti previsti dalla normativa antiriciclaggio (tra questi, banche e intermediari finanziari) devono effettuare la c.d. adeguata verifica della clientela, identificando preliminarmente ciascuno di essi per la prestazione dei propri servizi²⁹. L'onerosità degli obblighi di adeguata verifica della clientela aumenta, evidentemente, laddove il rischio di riciclaggio si presume sia più elevato. Ciò, ad esempio, accade ogni qualvolta il rapporto continuativo o l'operazione occasionale sia instaurato o effettuata a distanza (ciò che avviene, ad esempio, quando gli intermediari utilizzano Internet per la prestazione dei propri servizi). In tali circostanze, si rende necessaria quella che il Legislatore indica come "adeguata verifica rafforzata", dovendosi implementare misure di presidio specifiche ulteriori rispetto a quelle richieste usualmente in presenza del cliente³⁰.

Grazie alla diffusione di tecnologie sempre più avanzate, si è ampliato per gli intermediari il novero di tecniche per esperire l'adeguata verifica, anche in caso di adeguata verifica a distanza. Come evidenziato nello studio svolto in materia dalle tre

²⁷ BANCA D'ITALIA (2017), *Fintech in Italia. Indagine conoscitiva sull'adozione delle innovazioni tecnologiche applicate ai servizi finanziari*, Dicembre 2017.

²⁸ Come noto, quale misura di antiriciclaggio e contrasto al finanziamento del terrorismo, i soggetti obbligati, e tra questi le banche e gli intermediari finanziari, sono tenuti a procedere all'adeguata verifica del cliente, identificandolo in occasione dell'instaurazione di un rapporto continuativo o del conferimento dell'incarico per l'esecuzione di una prestazione professionale – e a determinate condizioni, in occasione altresì dell'esecuzione di un'operazione occasionale (cfr. articolo 17 ss. del decreto legislativo 21 novembre 2007, n. 231, come modificato e aggiornato a seguito del recepimento in Italia della direttiva (UE) 2015/849 (c.d. "IV Direttiva Antiriciclaggio").

²⁹ Articolo 17 ss. del decreto legislativo 21 novembre 2007, n. 231, come modificato e aggiornato a seguito del recepimento in Italia della direttiva (UE) 2015/849 (c.d. "IV Direttiva Antiriciclaggio") (il "D.Lgs. 231/2007")

³⁰ Ai sensi dell'art. 24 del D.Lgs. 231/2007, lo svolgimento dell'adeguata verifica rafforzata, richiesto in presenza di un elevato rischio di riciclaggio o di finanziamento del terrorismo, si adempie acquisendo informazioni aggiuntive sul cliente e sul titolare effettivo, approfondendo gli elementi posti a fondamento delle valutazioni sullo scopo e sulla natura del rapporto e intensificando la frequenza dell'applicazione delle procedure volte al controllo costante.

Autorità di vigilanza di settore (*i.e.* European Banking Authority – EBA, European Securities and Markets Authority – ESMA, European Insurance and Occupational Pensions Authority – EIOPA, congiuntamente “ESAs”), gli intermediari creditizi e finanziari utilizzano oggi tecniche che includono il riconoscimento facciale e la rilevazione di parametri biometrici, rendendo possibile lo svolgimento della verifica in tempi brevi ed agevolandone lo svolgimento anche qualora il cliente dovesse avvalersi di canali online di vendita. Tali strumenti, pertanto, permettono agli operatori di rivedere le modalità tradizionali di condurre le dovute verifiche sulla base degli standard tecnologici più innovativi, efficientando e velocizzando i processi e offrendo al cliente un servizio in linea con le aspettative di innovazione digitale³¹. A tal riguardo, le Autorità europee di vigilanza hanno auspicato un coordinamento tra le differenti Autorità nazionali al fine di introdurre un quadro regolamentare di secondo livello che tenesse in considerazione tali innovative modalità di svolgimento dell’adeguata verifica e che fosse il più possibile omogeneo.³² Sulla scia di tale riflessione, Banca d’Italia, nell’aprile 2018, ha proposto in consultazione di includere nell’ambito delle nuove disposizioni in materia di adeguata verifica della clientela la possibilità di utilizzare, in caso di adeguata verifica a distanza, “*meccanismi di riscontro basati su affidabili soluzioni tecnologiche innovative (quali, ad esempio, quelle che prevedono forme di riconoscimento biometrico)*”, *nella misura in cui fossero implementati robusti presidi di sicurezza*³³.

Tali soluzioni innovative si affiancano alla diffusione dell’Internet of Things nel mondo regolamentato. Si sta assistendo, ad esempio, al fenomeno della c.d. “Smart Finance”, la possibilità di monitorare in tempo reale lo stato di avanzamento dei lavori di determinati progetti di energy financing e real estate e di associarne la positiva concessione dei relativi finanziamenti.³⁴

Peraltro, l’*Internet of Things* ha conosciuto un notevole sviluppo nell’ambito del settore assicurativo, dal momento che le proprie caratteristiche e finalità ben si adattano alla struttura e alle finalità del c.d. “*InsurTech*”. Sono sorte soluzioni innovative in grado di

³¹ ESAS (2018), *Opinion on the use of innovative solutions by credit and financial institutions in the customer due diligence process*, JC 2017 81, 23 January 2018.

³² ESAS (2018), *Opinion on the use of innovative solutions by credit and financial institutions in the customer due diligence process*, JC 2017 81, 23 January 2018.

³³ BANCA D’ITALIA (2018), *Disposizioni in materia di adeguata verifica della clientela, Documento per la consultazione*, pag. 16, Aprile 2018. Al riguardo si ricorda che la consultazione in oggetto non si è ancora conclusa.

³⁴ COMMISSIONE EUROPEA (2013), *Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination, Final Report, A study prepared for the European Commission, DG Communications Networks, Content & Technology*, 2013/0037. Al riguardo, si confronti altresì EUROPEAN COMMISSION (2016), *Annex Accelerating clean energy in buildings to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, the Committee of the Regions and the European Investment Bank*, Brussels, COM(2016) 860 final, 30.11.2016.

rispondere alle esigenze del mercato in termini di efficienza, velocità di reperimento di informazioni e dati, al fine di costruire prodotti assicurativi personalizzati.

Si sono diffusi prodotti assicurativi “connessi” nell’ambito dei settori casa, *automotive* e salute, delineandosi le cd. “*smart home*”, “*smart car*” e “*smart health*”³⁵.

In particolare, con riferimento alle “*smart home*”, gli strumenti connessi raccolgono e trasferiscono dati che, oggetto di monitoraggio, sono utilizzati per comprendere le modalità di utilizzo e abbinano, personalizzandole, le polizze assicurative più idonee³⁶. Ugualmente, nelle “*smart cars*” sono impiantate le cc.dd. “scatole nere” che monitorano le modalità di guida e raccolgono dati su eventuali incidenti avvenuti³⁷. Infine, la strumentazione medica indossata dai pazienti raccoglie e trasmette dati relativi allo stato di salute, al funzionamento dello strumento stesso e possono in tal modo adattare l’offerta di polizze assicurative³⁸.

4. Conclusioni

La crescita e la diffusione del fenomeno *Internet of Things* stanno aumentando in misura esponenziale anche nel settore *FinTech* al fine di ampliare l’offerta di prodotti alla clientela e introdurre un approccio di *business* maggiormente dinamico, soprattutto dal punto di vista dell’offerta di una migliore *customer experience*.

In tale ambito, gli evidenti risvolti di carattere regolamentare, rendono necessario un continuo aggiornamento da parte dei soggetti vigilati che si rivolgano a questo tipo di strumenti. Con il generale processo di digitalizzazione in corso, l’avvento di nuove tecnologie (ad esempio il sempre più diffuso utilizzo di tecnologie *blockchain*) e l’ingresso nel mercato dei servizi finanziari di alcune *BigTech Companies*, è sempre più evidente l’esigenza di accompagnare a ogni nuova prassi un’estensiva analisi di conformità regolamentare.

In tale contesto, la sussistenza di linee guida per gli operatori del settore agevolerebbe la crescita e lo sviluppo di soluzioni innovative in maniera maggiormente armonizzata nel mercato. Un quadro regolamentare ben definito, infatti, renderebbe possibile efficientare il processo di innovazione assicurando, al tempo stesso, la tutela del cliente. Il percorso è ancora in corso di definizione, sorretto dagli impulsi del mercato che spesso anticipa le proposte del Legislatore. Non è un caso, infatti, che il fenomeno dell’*Internet of Things* non abbia ancora trovato una piena e concreta regolamentazione, almeno nel settore *FinTech*. Regolamentazione che, in ogni caso, è sicuramente auspicabile nella

³⁵ COMMISSIONE EUROPEA (2013), *Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination, Final Report, A study prepared for the European Commission, DG Communications Networks, Content & Technology*, 2013/0037.

³⁶ EIOPA (2018), *EIOPA InsurTech Roundtable. How technology and data are reshaping the insurance landscape*, EIOPA-BoS/17-165, 05 July 2017.

³⁷ EIOPA (2018), *Sixth Consumer Trends Report*, ISSN 2467-3714.

³⁸ IAIS (2017), *FinTech developments in the Insurance Industry*, 21 February 2017.

misura in cui sia in grado di supportare il progresso tecnologico, al tempo stesso, superando le asimmetrie informative tra operatori tecnologici e clientela che ancora oggi sussistono in tale ambito. In tal senso, un lodevole esempio è costituito dalla recente normativa in materia di servizi di pagamento che con la Direttiva PSD2 e la regolamentazione tecnica connessa, ha rappresentato forse il primo tentativo di “regolamentazione della tecnologia” nel settore dei servizi finanziari³⁹.

³⁹ Cfr. Cascinelli-Pistoni, *La Direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno*, in *Dir. Banc.*, 28 luglio 2016.