**ALMA MATER STUDIORUM - UNIVERSITÀ DI BOLOGNA**

**CAMPUS DI CESENA**

**Scuola di Scienze**

**Corso di Laurea in Ingegneria e Scienze Informatiche**

# INTERNET OF THINGS NELLA SOCIETÀ: AMBITI APPLICATIVI E PROBLEMATICHE

Relazione finale in

**PROGRAMMAZIONE DI SISTEMI EMBEDDED**

Relatore

**Prof. Alessandro Ricci**

Presentata da

**Giacomo Pasini**

Correlatrice

**Prof.ssa Claudia Cevenini**

Sessione I

Anno Accademico 2017/2018

## Sommario

# Introduzione

Con il termine Internet delle Cose (*Internet of Things, IoT*) si indica la rete di dispositivi dotati di sensori, attuatori, software e connettività che gli permette di digitalizzare informazioni sull'ambiente circostante e comunicare tra loro scambiando dati attraverso Internet. Questa tecnologia ha iniziato ad essere largamente impiegata negli ultimi anni, grazie ad un insieme di fattori che ne hanno favorito la diffusione; tuttavia già da prima del 2009, quando il termine cominciò ad essere utilizzato con il suo significato attuale[1], esistevano tecnologie che adoperavano la comunicazione tra calcolatori (*Machine to Machine, M2M*), molte delle quali si sono poi evolute per sfruttare le capacità di connettività offerte dal protocollo IP e dal web.

Oggi, grazie al sempre più rapido sviluppo di tecnologie IoT, esistono sistemi sempre più complessi capaci di sfruttare al meglio il potenziale dei dati che generano e che si scambiano con altri sistemi in diversi ambiti, migliorando l'efficienza dei processi e abbassando il costo di beni e servizi. Per arrivare a questo livello di sviluppo si è dovuta attraversare una progressione di diversi stadi dei prodotti IoT dove inizialmente, in modo simile a come accadde nei primi anni della nascita di Internet e dei siti web, non era molto chiaro quale sarebbe stato il ruolo finale che questi prodotti avrebbero avuto nel mercato, se come oggetti semplicemente più intelligenti e capaci grazie all'elettronica incorporata o come qualcosa di più complesso, basato sulla comunicazione tra molteplici sistemi IoT per favorire l'aggregazione di diversi tipi di dati per derivarne sempre più conoscenza riguardo l'ambiente circostante e prescrivere compiti da eseguire in modo automatizzato e con il minimo intervento umano.

Per chiarire meglio il processo evolutivo che ha portato alla nascita di IoT come lo conosciamo oggi e per riflettere sui possibili utilizzi futuri è necessario analizzare i vari stadi della sua evoluzione e le condizioni e le necessità che ne hanno favorito lo sviluppo.

[1] http://www.rfidjournal.com/articles/view?4986

# L’evoluzione dei sistemi IoT

I dispositivi IoT come li conosciamo oggi sono già molto differenti rispetto ai primi prodotti (*smart objects*) che apparivano sul mercato qualche anno fa: sono il risultato di un insieme di evoluzioni sia nella tecnologia che impiegano, ovvero sensori, connettività e firmware, che nel modo di percepire la funzionalità che dovrebbero avere per raggiungere il loro massimo potenziale, basata principalmente sulla generazione, condivisione e aggregazione di diversi insiemi di dati per garantire la massima interazione sia tra prodotti che tra sistemi di prodotti IoT. Per descrivere questo cambiamento e comprendere quale sarà l’impiego che avranno in futuro è utile analizzare le fasi principali della loro evoluzione.

## L’evoluzione di IoT da M2M

Il concetto di comunicazione tra calcolatori non è nuovo ed è da molto tempo impiegato nell’industria, dove i macchinari addetti ad un processo sono capaci di scambiarsi informazioni riguardo il loro stato in modo autonomo e con il minimo input da parte dell’operatore. Nei sistemi M2M, la novità consisteva nella comunicazione a due vie tra macchinari, tipicamente in real-time, che gli consentiva di poter intraprendere autonomamente azioni in base agli stati rilevati dagli altri dispositivi. La principale differenza che però separa i più datati sistemi basati su M2M da quelli IoT odierni è la generale incapacità di poter sfruttare il potenziale dei dati che raccolgono dai vari sensori: il focus resta sui dispositivi e sul software che svolge il processo e i dati generati sono concepiti per essere trasmessi ed utilizzati all’interno della specifica applicazione che l’impianto in questione deve svolgere, formando un ambiente relativamente chiuso e con gestione centralizzata. Lo scopo principale delle informazioni raccolte era fornire servizi di diagnostica e allerta in real-time, per poi essere scartate quando considerate inutili per il contesto attuale; mancava la consapevolezza del potenziale che i dati potevano fornire se riutilizzati in un contesto più ampio, ad esempio se aggregati a quelli di altri sistemi collegati attraverso una rete. Grazie ai progressi della tecnologia nella telecomunicazione e nell’elettronica e all’avvento del World Wide Web verrà data la possibilità di creare sistemi con queste caratteristiche, permettendo ai dati di uscire dai classici sistemi centralizzati, chiusi e poco interconnessi e di sfruttare il potenziale di Internet, seguendo i suoi principi di decentralizzazione, flessibilità e collaborazione.

## Condizioni favorevoli alla nascita di IoT

A differenza dell'architettura su cui si basano i sistemi precedentemente descritti, incentrata su una precisa applicazione da svolgere, l'implementazione di soluzioni IoT si basa sulla flessibilità e sulla modularità: essendo un'infrastruttura caratterizzata da un controllo decentralizzato e dall'estendibilità si ha la consapevolezza che nel tempo sarà soggetta a diversi cambiamenti ed estensioni, vista la varietà di dispositivi che vi dovranno interagire e per i quali si dovrà garantire interoperabilità. In questo senso l'aspetto più importante è l'astrazione tra i vari layer dell'architettura in modo da favorire il più possibile la modularità per le funzioni svolte.

Con IoT il focus si sposta sui dati: si ha la consapevolezza che sfruttare i dati generati per aggregarli ed analizzarli permette di scoprire importanti correlazioni e di generare valore; di conseguenza è necessario essere in grado di poterne gestire di ogni tipo e anche di non strutturati, i quali risultano scarsamente compatibili con i classici database relazionali, che divengono inefficienti per quell'ambito di utilizzo. La principale differenza rispetto ad un'architettura M2M è quindi la dissociazione dei dati dalla loro fonte e da una specifica applicazione: diventano significativi relativamente al contesto in cui vengono utilizzati.

Lo sviluppo delle tecnologie IoT ha subito una forte spinta dovuta ad una congiunzione di situazioni favorevoli che hanno reso la realizzazione di queste infrastrutture possibile, soprattutto in termini di costi: negli ultimi anni, grazie ai costanti progressi nella tecnologia, il costo della produzione di chip e sensori è calato a tal punto da permettere di incorporare negli oggetti processori in grado di realizzare tutte le funzioni richieste da una moderna architettura IoT, insieme ad una capacità di storage in grado di supportare la mole di dati che i dispositivi potrebbero scambiarsi, il tutto a prezzi sempre più bassi e di conseguenza più accessibili ai consumatori. In modo simile ai prezzi associati all'elettronica, anche la connettività ha subito una drastica diminuzione dei costi rispetto a soli pochi anni prima: nonostante le tecnologie di comunicazione siano sempre state a disposizione anche dei sistemi M2M, in passato il costo per implementare una connessione tra dispositivi su larga scala sarebbe risultato quasi improponibile; tuttavia, con il passare del tempo l'utilizzo di queste tecnologie si è fatto sempre più frequente, facendo crollare i prezzi per le connessioni su rete cellulare e satellitare, favorendo quindi lo sviluppo di tecnologie di comunicazione su larga scala ideali per implementazioni IoT.

A tutto questo si deve aggiungere il calo dei prezzi relativi allo storage, caratteristica fondamentale per poter gestire i crescenti flussi di dati grazie anche allo sviluppo e all'adozione di servizi cloud, che forniscono alle aziende servizi

pronti per il processamento e lo storage di dati in rete; oltretutto, il cloud è un componente fondamentale per un'architettura IoT ideale. Oltre ai problemi di costo per lo storage, il modo in cui i dati vengono processati e raccolti è un altro problema che si è dovuto affrontare, essendo la chiave per poterne ottenere il massimo valore: dovendo gestire enormi flussi di informazioni, un controllo centralizzato per un'architettura IoT risulta inefficiente e l'estensione delle capacità di storage per tenere il passo con la crescente mole di dati non è conveniente. Per questo si è reso necessario lo sviluppo di database distribuiti, gestiti logicamente come un solo file system ma fisicamente come cluster separati, permettendo di distribuire i dati in diversi modi ed eliminando il problema della scalabilità; a tutto questo si devono aggiungere gli sviluppi negli algoritmi di gestione dei flussi di dati per favorirne la distribuzione parallela in real-time, caratteristica fondamentale in quanto la maggior parte delle applicazioni IoT ha bisogno di operare non solo su dati storici, ma anche generati in tempo reale per poter intraprendere azioni automatizzate di risposta agli eventi.

L'evoluzione per i database riguarda anche nuovi modi di gestire i diversi tipi di dati generati dai dispositivi al giorno d'oggi, difficilmente compatibili con i classici database relazionali per via della loro eterogeneità: basti pensare alla necessità di dover integrare milioni di dispositivi differenti in cui ogni categoria di prodotti è potenzialmente dotata di una sua struttura per gestire i dati, oppure alla gestione efficiente di file audio e video. Di conseguenza i database relazionali continueranno ad avere il loro classico ruolo per quanto riguarda il trattamento di dati strutturati e prevedibili, ma per le altre categorie si dovranno integrare soluzioni adatte a gestirli in modo indipendente dalla loro struttura, come ad esempio NoSQL.

## Le fasi di sviluppo dei prodotti IoT

Anche i dispositivi IoT hanno subito diversi cambiamenti nel corso degli anni, subendo modifiche alla loro implementazione mentre col tempo i produttori realizzavano quali erano le caratteristiche ideali di cui dovevano essere dotati. Si possono distinguere diverse fasi relative alla crescita di questi prodotti, partendo da quella di *smart object*: un dispositivo diventa programmabile e quindi più capace grazie alla capacità di eseguire semplici calcoli per rispondere ai comandi dell'utente o adattarsi automaticamente a certe condizioni esterne, grazie agli stati rilevati dai sensori. Il passo successivo è l'aggiunta della connettività: il dispositivo diventa controllabile a distanza grazie all'accesso ad Internet; questo passaggio è importante perché la visualizzazione dello stato del dispositivo da remoto ha permesso ai fornitori di comprendere l'importanza e l'efficienza derivata dallo

sfruttamento dei dati generati: le funzioni di monitoraggio a distanza non sono solo utili al consumatore, ma permettono al fornitore di poter eseguire manutenzione predittiva sui loro prodotti, potendo verificarne lo stato in tempo reale, migliorando in modo significato la qualità del servizio.

La fase successiva consiste nello sviluppo di sistemi formati da più prodotti che si occupano di funzioni simili, come ad esempio nella gestione delle abitazioni, dove i vari dispositivi intelligenti come il termostato, il frigorifero e gli altri elettrodomestici sono interconnessi e si scambiano dati con lo scopo di migliorare l'efficienza nella gestione della casa, aggregando le informazioni utili per trarne conclusioni sulle azioni da intraprendere in modo autonomo, oltre ad essere gestibili direttamente dalla rete attraverso applicazioni su misura per il sistema.

A questo punto era chiaro che i prodotti per funzionare al massimo delle loro potenzialità avevano bisogno di comunicare il più possibile con l'ambiente circostante, senza limitare lo scambio di dati a una semplice comunicazione con il fornitore riguardante il loro stato ma condividendo dati utili con altri sistemi che potrebbero averne bisogno; così nacquero diversi sistemi di prodotti per contendersi questo mercato, proponendo soluzioni simili anche per l'ambito industriale. La caratteristica che separa questa fase da quella precedente sta nel fatto che questi sono progettati sin dall'inizio per contemplare la loro inclusione e comunicazione in sistemi più grandi, in modo diverso dal semplice scambio di dati all'interno del dominio del solo fornitore.

L'ultima fase riguarda la comunicazione tra diversi insiemi di dispositivi, ovvero l'aggregazione di dati provenienti da diversi servizi, come quelli per la gestione della casa, il sistema operativo della macchina o qualsiasi altro dispositivo *wearable*, in modo da poter raccogliere più dati possibili per riuscire a scoprire pattern utili a migliorare ancora di più l'efficienza e la qualità dei servizi. Questo rappresenta un'impresa difficile per molte compagnie, in quanto nonostante preferirebbero mantenere il controllo sui dati generati dai loro prodotti, che gli consente di avere una semplificazione nella loro gestione e anche un vantaggio generale rispetto alla concorrenza, sono tuttavia obbligati nella pratica a doverli condividere in parte con altri sistemi per poter restare in competizione, creando di conseguenza dibattiti riguardo la gestione e il possesso dei dati.

I problemi sul controllo delle informazioni in questione sono principalmente di natura commerciale ed economica, in quanto si teme che lo sfruttamento dei dati da parte di una compagnia che sviluppa servizi per i sistemi di prodotti possa portare un ingiusto svantaggio ai danni, ad esempio, delle aziende che producono i singoli dispositivi che possono interagirvi. Da un punto di vista puramente tecnologico, invece, un problema del genere potrebbe essere risolvibile se i sistemi IoT venissero implementati su un'architettura capace di propagare i dati e

distribuirli a chi li richiede e nella forma in cui vengono richiesti, adeguata all'ambito specifico in cui verranno utilizzati; in questo modo le aziende si potrebbero accordare tramite contratto per ricevere la vista sui dati di cui hanno bisogno, e i fornitori potrebbero continuare a ricevere i dati utili ai loro scopi tipici.

Per chiarire meglio le potenzialità di questi sistemi e l'importanza del ruolo che i dati assumono quando vengono aggregati e condivisi con altri dispositivi è utile analizzare in che modo possono provvedere a migliorare l'efficienza dei procedimenti, grazie soprattutto all'integrazione con altre tecnologie.

## Integrazione di IoT con Big Data

Le prime implementazioni di tecnologie IoT avevano come scopo principale, almeno dal punto di vista del fornitore del prodotto, il monitoraggio dei sistemi basato sull'invio di segnali da parte della macchina per dare informazioni sullo stato rilevato dai sensori, permettendogli di poter controllare lo stato attuale del dispositivo e provvedere eventualmente ad una manutenzione; queste funzionalità sono poi diventate sempre più realizzabili ed efficienti grazie alla crescita delle reti wireless e alla possibilità di monitorare i dati in tempo reale, che ne ha permesso l'implementazione anche in sistemi fortemente dipendenti da continui cambiamenti dell'ambiente esterno, come ad esempio nei mezzi di trasporto. I sistemi sono poi diventati più complessi, evolvendosi nelle loro capacità computazionali, non più limitate alla semplice lettura dei loro sensori e invio di segnali ma implementando una comunicazione di tipo *duplex*, permettendo ai produttori di poter interagire direttamente e a distanza inviando messaggi ai dispositivi per far fronte alle segnalazioni inviate, comunicare azioni da intraprendere ed eventualmente gestire gli aggiornamenti del software; la necessità di poter effettuare operazioni di controllo da remoto ha quindi accelerato ulteriormente lo sviluppo di dispositivi sempre più capaci.

Avendo a disposizione sistemi più complessi che generano sempre più dati, il focus è passato dal gestirli all'interno di un'applicazione specifica all'utilizzarli anche per scopi esterni al sistema, per poter derivare informazioni utili attraverso la loro analisi anche in altri contesti per migliorare efficienza e produttività. In questo modo, mentre prima si osservava un sistema per capirne lo stato attuale in modo da poterne gestire meglio la manutenzione, grazie alla mole di informazioni a disposizione è diventato possibile gestire possibili casi futuri effettuando manutenzione predittiva, facilitata dalla raccolta di dati più arricchiti grazie alle segnalazioni inviate da migliaia di dispositivi, anche in tempo reale, causando un'ulteriore minimizzazione dei costi. Un successivo potenziamento di questi

metodi prevede l'integrazione di queste grandi quantità di dati con l'automazione dei procedimenti, per non limitarsi solo al prevedere cosa potrà succedere, ma anche prescrivendo al sistema una serie di azioni da intraprendere autonomamente ed in tempo reale per reagire alle mutate condizioni, con lo scopo di renderlo adattabile e in grado di reagire in modo autonomo grazie alle sempre più ricche informazioni a disposizione che contribuiscono a fornire una vista più precisa dello stato del sistema.

La gestione di dataset di grandi dimensioni per derivarne informazioni utili prende il nome di *Big Data* ed è caratterizzata dalla necessità di sfruttare una quantità di dati tale da rendere quasi inadeguate le attuali tecnologie, necessitando di soluzioni in grado di gestire tutti gli aspetti legati alla cattura, allo storage, alla trasmissione in tempo reale e all'analisi di elevate quantità di informazioni di diversa struttura. I sistemi IoT moderni devono essere in grado di svolgere tutti questi compiti per fornire i servizi descritti; lo sviluppo di tecnologie legate ai Big Data è fortemente correlato alla loro evoluzione: basti guardare allo sviluppo di database non relazionali per far fronte alla diversa struttura dei dati trattati, o al costante miglioramento delle reti wireless, che devono poter trasferire una quantità di informazioni crescente in modo esponenziale con lo sviluppo di IoT.

Gli elementi caratterizzanti fondamentali dei Big Data sono *volume*, *varietà* e *velocità*. Il volume dei dati, crescente esponenzialmente a causa del sempre maggiore numero di dispositivi in comunicazione, è indicativo del fatto che per analizzarli e trasmetterli è necessario provvedere al loro storage, realizzando soluzioni adeguate in termini di capacità di memoria e di gestione dei database. La varietà riguarda invece la loro struttura che può assumere varie forme, non solo testuali e numeriche come lo erano per la maggior parte in passato ma anche audio, video, immagini e altro: sono quindi necessari database che non siano legati ad una precisa strutturazione delle informazioni, insieme a metodi efficienti per ricavarne relazioni utili all'analisi. La velocità si riferisce all'ovvia constatazione che enormi dataset possono aver bisogno di essere gestiti con elevata rapidità se si vuole dargli valore in un certo contesto, specialmente se legati a processi di analisi o automazione la cui efficienza può dipendere fortemente dai dati ricevuti entro un certo lasso di tempo.

Per chiarire i benefici relativi all'analisi dei dati, specialmente se aggregati e confrontati in tempo reale ed eventualmente da più sorgenti, è bene descrivere i principali metodi di analitica i cui processi si evolvono insieme a queste tecnologie per trarne valore.

### *Analitica descrittiva, predittiva e prescrittiva*

I processi legati all'analitica si sono evoluti, spinti dalle possibilità date dall'analisi dei Big Data, e possono essere catalogati in base ai risultati che forniscono. Il processo più basilare relativo all'analisi dei dati è noto semplicemente come diagnostica, o *Business Intelligence* in ambito aziendale, dove un qualsiasi tipo di dati relativo ad un prodotto o procedimento viene analizzato con lo scopo di ricavare informazioni aggiuntive utili per valutare o migliorare le decisioni strategiche da prendere a riguardo. Grazie all'avvento dei Big Data si possono distinguere tre fasi successive riguardanti l'analitica.

L'operazione principale che può essere tipicamente svolta sui dati è l'analitica descrittiva, ovvero l'analisi che fornisce come output una descrizione dello stato, attuale o passato, di un sistema o dispositivo. L'aumentare della quantità e della varietà dei dati permette di effettuare analitica predittiva, che offre informazioni volte a prevedere gli stati futuri in cui si potrà trovare il sistema grazie al processamento di dataset attuali o storici, integrati eventualmente con appositi algoritmi e *Machine Learning* per evidenziare pattern comuni utili nei procedimenti da seguire: l'obiettivo di questi procedimenti è cercare di capire cosa potrà succedere in futuro.

Il passo successivo riguarda l'analitica prescrittiva ed è un potenziamento delle tecniche precedenti, con la differenza che i dati utilizzati sono per la maggior parte analizzati in contesti real-time in quanto le capacità predittive vengono utilizzate per istruire il sistema (dotato per lo scopo di appropriate tecnologie quali complessi algoritmi e Machine Learning) in modo da consentirgli di valutare, in base ad una serie di fattori tra cui il possibile rischio, delle azioni da intraprendere autonomamente per adattarsi ai cambiamenti e portare ad uno scenario futuro ideale per il processo da svolgere. La differenza sostanziale di quest'ultimo procedimento consiste nella sua dipendenza non solo dalle informazioni disponibili in tempo reale, ma anche dai dati esterni al sistema, che diventano nella maggior parte dei casi fondamentali per la corretta interpretazione dei fattori che potrebbero influenzare lo svolgimento delle operazioni: un esempio per questo caso è rappresentato dalla macchina dotata di guida autonoma, che per il raggiungimento dello scopo ha bisogno di analizzare non solo i dati generati internamente al proprio sistema (riguardanti ad esempio lo stato del serbatoio o la condizione dei freni), ma anche quelli provenienti dall'ambiente esterno quali le informazioni sulla strada, la posizione delle altre macchine e le condizioni meteo.

## L’architettura ideale per i sistemi IoT

Per implementare un’architettura IoT che sia in linea con i principi di collaborazione e condivisione delle informazioni per i quali è intesa, è fondamentale l’adozione di uno standard condiviso. Si può affermare che la priorità in termini di funzionalità dovrà consistere nel garantire ad ogni soggetto di poter accedere ai dati di cui necessita per svolgere le proprie funzioni: le imprese che si occupano della gestione dell’interazione tra i sistemi non dovrebbero privare gli eventuali produttori dei singoli dispositivi della possibilità di effettuare tutte le operazioni che svolgevano in precedenza attraverso i dati che elaborano, come poteva succedere prima dell’arrivo sul mercato dei sistemi di sistemi; allo stesso modo gli utenti non dovrebbero vedersi privati dell’autonomia nella gestione delle informazioni che hanno potuto sperimentare sin dalle prime fasi dei prodotti IoT.

Un esempio di come i sistemi complessi dipendano fortemente dalla condivisione può essere dato da una smart city: si pensi alla necessità di un sistema di sorveglianza cittadina intelligente di dover utilizzare i dati sull’illuminazione, o quelli sulle condizioni meteo e sul traffico; oppure si pensi ad un sistema di gestione stradale intelligente che ha bisogno a sua volta di accedere ai dati sopracitati per poter informare correttamente i guidatori. In questi e molti altri casi la disponibilità delle informazioni è fondamentale, e l’esclusione dei sistemi dalla loro condivisione pregiudicherebbe il funzionamento di ognuno di essi; ne segue che la collaborazione è la chiave, ed il dibattito sulla proprietà dei dati è da intendere come un dibattito relativo al loro controllo.

Garantire l’adeguato controllo sui dati ad ogni figura facente parte di un processo IoT, favorendo la collaborazione e la condivisione e rispettando al contempo i regolamenti sulla privacy e sulla sicurezza che devono caratterizzare questi sistemi è una sfida molto complicata, di tipo sia tecnologico che sociale ed economico, ed è destinata a creare molti dibattiti, soprattutto relativi all’adozione di standard che dovranno essere accettati e condivisi il più possibile. Nel caso di IoT è però presente un lato positivo che può facilitare la questione: la propagazione dei dati ai vari richiedenti ha un costo marginale quasi zero, permettendo a tutti di ottenere ciò di cui hanno bisogno senza che la cosa costituisca un particolare svantaggio per gli altri; i problemi sono quindi concentrati quasi esclusivamente nella progettazione dell’architettura standard.

## Caratteristiche principali

Prima di introdurre il modello di architettura proposto, denominato *First Receiver*, è necessario considerare alcune delle caratteristiche che si può assumere saranno in ogni caso presenti in qualsiasi soluzione futura, per motivi di elevata sinergia e compatibilità di queste tecnologie con le proprietà tipiche dei sistemi IoT.

### *Edge Computing*

L'*Edge Computing* rappresenta un'estensione e un miglioramento del cloud computing in particolare per l'ambito IoT, con lo scopo di ottimizzare la latenza di rete e la rapidità di elaborazione dei dati togliendo parte del controllo sulle funzionalità ai nodi centrali della rete e distribuendolo ai suoi confini, logicamente in diretto contatto con i dispositivi fisici. In questa architettura i dati raccolti dai loro sensori vengono analizzati e processati il più vicino possibile alla sorgente, distribuendo in modo più ottimale i calcoli e permettendo di svolgere sul posto delle operazioni di correzione, strutturazione o compressione, di effettuare le operazioni di analitica e di scartare eventuali dati ripetitivi o non necessari, alleggerendo di conseguenza il carico di rete per il data center centrale del cloud. Si utilizza in particolare per sistemi che sono fortemente dipendenti dall'ambiente che li circonda e che quindi devono assicurare un'elevata qualità di servizio fornendo una risposta in real-time al mutare delle condizioni esterne, come può essere nel caso di un'automobile o di un ambiente industriale, dove un'implementazione che si basa su un processamento dei dati più vicino al punto di raccolta può fare la differenza in termini di affidabilità.

Di seguito sono elencate le funzionalità che verrebbero svolte da un edge device associato ad un sistema basato sul modello del First Receiver:

- **Configurazione dei sensori**: Riguarda la gestione delle operazioni di configurazione che risulterebbero generalmente troppo pesanti per essere svolte singolarmente per ogni sensore: distribuire sull'edge device eventuali calcoli necessari alla gestione gli permetterebbe di essere più semplici ed appropriati al compito che devono svolgere.
- **Ricezione dei messaggi**: Viene effettuata la raccolta delle rilevazioni per poter effettuare operazioni di calcolo preliminari che possono comprendere l'analisi, l'aggregazione di dati complementari o la strutturazione in forme più adatte alle fasi successive.
- **Gestione dei protocolli di comunicazione**: Esistono diversi tipi di sensori, applicazioni o web service basati su diversi protocolli più o meno sofisticati: è

quindi necessario poter tradurre i dati in forme compatibili con essi per poter garantire l'interoperabilità.

- **Filtraggio dei messaggi**: È fondamentale rimuovere in modo preventivo qualsiasi messaggio del flusso di eventi che risulta non necessario o ripetitivo ai fini delle applicazioni, come ad esempio valori segnalati costantemente dai sensori anche in assenza di cambiamenti.
- **Notifica e triggering di eventi**: Un'operazione caratterizzante di ogni sistema IoT riguarda la segnalazione di situazioni particolari in base alla ricezione degli appropriati segnali dai sensori, oltre all'innesco di eventi per svolgere azioni a riguardo.
- **Potenziamento della sicurezza**: L'edge device è il dispositivo ideale per implementare un ulteriore layer di sicurezza che funga da firewall tra i dispositivi e la rete.

### *Architettura event-driven e publish-subscribe*

Le scelte implementative che attribuiscono maggiore scalabilità ad un sistema IoT sono sicuramente quelle basate sulla gestione degli eventi e sulla separazione della creazione dei messaggi dalla loro consumazione, in quanto entrambe sono la migliore rappresentazione logica di come le informazioni scambiate tra i dispositivi vengono ricevute ed utilizzate. In primo luogo, la raccolta di un dato da parte di un sensore rappresenta un evento che avviene in un certo istante di tempo: da qui la gestione delle informazioni come flussi di eventi generati. In secondo luogo, come i dati vengono successivamente utilizzati può variare anche di molto in base all'uso che ogni richiedente ne vuole fare; va ricordato che la caratteristica principale dei sistemi IoT moderni, in opposto al passato, sta nello sfruttamento del valore che i dati possono assumere in situazioni anche molto diverse tra loro. Per questo si rende necessario separare il più possibile la creazione dei dati dal loro utilizzo, per permettere la riusabilità e per impedire il verificarsi di sistemi relativamente chiusi e con una logica di consumazione che vede i dati segregati all'interno di una specifica applicazione.

## Il modello del First Receiver

Lo scopo dell'architettura First Receiver è quello di garantire ad ogni utilizzatore che fa parte del processo di poter trarre dai dati il massimo potenziale. Per quanto riguarda la conformità legale dei trattamenti di eventuali dati personali presenti nei sistemi, si suppone che la base giuridica sia costituita dal contratto che verrà logicamente stipulato tra i fornitori di dispositivi e servizi ed i loro utilizzatori, tenendo conto che questa architettura trova la sua applicazione più indicata nella gestione di attività che richiedono un significativo livello di interazione tra dispositivi e l'intervento di più soggetti nel processo caratterizzati da diverse necessità. Una situazione tipica potrebbe essere, ad esempio, la gestione di un locale: un dispositivo di tipo First Receiver associato ad esso si occuperebbe di raccogliere i dati generati dalle applicazioni in uso rendendoli disponibili ai soggetti che ne richiedono la visione, nel formato, nei tempi e nei modi stabiliti dal contratto di utilizzo. Si possono individuare le seguenti figure che potrebbero ipoteticamente partecipare al processo:

- Gli impiegati, che visualizzano le informazioni generate dalle applicazioni presenti sui dispositivi del locale: queste possono essere raccolte dal First Receiver ed eventualmente elaborate e messe in relazione tra loro per garantire una vista più completa su tutto il sistema.
- L'ufficio di gestione del locale (o della catena a cui appartiene), che potrebbe aver bisogno di richiedere quei dati in forma aggregata e più adatta ai suoi scopi, che possono comprendere ad esempio l'analisi delle spese o della produttività.
- I fornitori dei prodotti IoT, che riceverebbero gli stessi dati che hanno sempre ottenuto per poter svolgere le operazioni di cui si occupavano in precedenza, che possono comprendere monitoraggio, manutenzione o supporto al software. Inoltre, sarebbe possibile accordarsi tramite contratto per lo scambio di altri dati che possono essere di altrettanta utilità: ad esempio, la correlazione tra lo stato dei loro dispositivi in relazione alla temperatura registrata, oppure al numero di persone presenti.
- I fornitori di prodotti del locale, a cui verrebbero comunicati i livelli attuali delle scorte in magazzino o lo stato dei prodotti in uso, per fornirgli un'indicazione su come e quando organizzare le consegne.
- Gli organi di controllo, che potrebbero adoperarsi in futuro per ottenere automaticamente dei report nel formato da loro richiesto sulla situazione dei dispositivi per verificarne la conformità ai regolamenti.

Oltre che delle caratteristiche di edge device descritte in precedenza, un dispositivo First Receiver dovrebbe comporsi delle seguenti funzionalità:

- **Storage dei dati**: Per poter processare le rilevazioni raccolte ed effettuare le appropriate operazioni di gestione prima di inoltrarle ai richiedenti, la presenza di un database locale è obbligatoria. In questo caso, trattandosi di un dispositivo intermediario, è necessario favorire l'efficienza utilizzando minime quantità di hardware e storage e garantendo la capacità di poter immagazzinare i dati allo stesso ritmo della loro generazione, il tutto contemplando un elevato rapporto di compressione. Per favorire l'automatizzazione dei procedimenti dovrà anche essere il più possibile indipendente, necessitando quindi di minime operazioni di gestione (ci saranno casi in cui la presenza di supporto tecnico esterno non sarà scontata); in ogni caso l'accesso al database dovrà essere facilitato dalla presenza di standard comuni (ad esempio MySQL).
- **Gestione del firmware**: Il First Receiver dovrà disporre dei metodi per scaricare ed applicare gli aggiornamenti dei dispositivi a cui è collegato, per garantire in ogni momento la sicurezza dell'ambiente applicativo.
- **Amministrazione dei dati**: Questa è la parte più importante, in quanto rappresenta lo strato di funzionalità atte a gestire il flusso di dati: saranno presenti delle applicazioni apposite per la loro amministrazione che si occuperanno di mettere in atto i permessi e le regole stabilite dai contratti tra i soggetti e dai regolamenti in materia (GDPR nel caso di trattamento di dati personali). I dati presenti nello storage locale del First Receiver potranno essere eventualmente manipolati solo dai soggetti che sono stati designati come responsabili delle sue operazioni; nell'ambito del GDPR le figure compatibili con essi possono essere quelle del responsabile del trattamento o di un incaricato alle sue dipendenze. Sempre supponendo un contesto in un vengono trattati dati di natura personale bisognerà contemplare il rispetto dei principi del trattamento e dei diritti degli interessati, il che si traduce, ad esempio, nella necessità di tenere traccia del periodo per il quale i dati vengono memorizzati per garantire che il tempo di conservazione non ecceda quelli necessari al conseguimento delle finalità stabilite nel contratto; inoltre, per gli stessi motivi di rispetto delle finalità bisognerà controllare l'invio dei dati ai soggetti richiedenti, minimizzandoli correttamente per adeguarli agli scopi che sono stati dichiarati.

## L’impatto di IoT nella società

Le tecnologie IoT odierne permettono di attingere ai Big Data e di sfruttare la loro analisi per aumentare efficienza e produttività, abbattendo progressivamente i costi marginali della produzione e della condivisione di innumerevoli beni e servizi. Questo è ciò che già da anni sta succedendo nel campo dell’informazione grazie all’avvento di Internet; basti pensare alla semplicità con cui oggi è possibile condividere qualsiasi contenuto multimediale nella rete, come ad esempio libri e articoli: non è più necessario affrontare i costi dovuti alla stampa e alla distribuzione e le idee possono essere condivise immediatamente nella rete ai soli costi di elaborazione e connessione di rete. Grazie all’avvento di una piattaforma tecnologica aperta e distribuita, che permette a qualsiasi entità che ne fa parte di interagire e comunicare per migliorare tutti gli aspetti della società, si è iniziato più che mai a riconoscere l’importanza della condivisione e della collaborazione, seguendo il concetto di un’economia collaborativa (*sharing economy*) in opposizione alla logica del profitto su cui si è sempre basata la società moderna, con la quale attualmente convive in modo ibrido e spesso conflittuale.

Questo nuovo paradigma si trova tuttavia in contrasto con la concezione di società a cui ci si è abituati finora: difatti, il capitalismo è stato pensato per far fronte ad un’economia basata sulla scarsità e di conseguenza si assume che sia sempre presente un mercato competitivo; in questa logica tutto è determinato dal mercato e l’obiettivo incoraggiato è quello di portare quasi ogni aspetto umano nella sfera economica per essere commercializzato e scambiato, il che spesso va a formare monopoli e oligopoli, che tendono a fissare prezzi più alti del loro valore effettivo per mantenere il controllo e sfavorire la concorrenza. In un’economia del genere il profitto viene fatto ai margini, dove ogni entità facente parte di un processo ha i suoi costi che ne giustificano la sua partecipazione; proprio questo è l’aspetto che la mette in contraddizione con un’economia collaborativa basata sullo scambio reciproco: grazie alle nuove tecnologie che oggi rendono possibile l’implementazione su larga scala di tale economia tramite la digitalizzazione e l’interconnessione nella rete, i costi marginali tendono sempre più allo zero. Se si estende questo ragionamento, si può immaginare una situazione in cui il costo di produzione di un bene o servizio diventa quasi nullo, raggiungendo una situazione ottimale: questo è l’obiettivo che il capitalismo si pone, ma il suo raggiungimento detterebbe l’inizio della sua scomparsa, vista l’impossibilità di ricavare ulteriore profitto.

Naturalmente c’è da considerare l’intenzione dei monopoli di mantenere il loro controllo, che si traduce nel proteggere gli investimenti svolti per il maggior tempo possibile, sfruttando il potere acquisito per manipolare i prezzi e rallentare sia

eventuali contendenti che la diminuzione dei costi marginali. Questi tentativi, per quanto efficaci nel breve periodo, tendono tuttavia a non durare per sempre: specialmente in questo caso, con la rivoluzione tecnologica basata sull'architettura IoT, i vantaggi relativi al suo utilizzo sono talmente elevati che l'unico modo per i monopoli per tenere testa a questo fenomeno è investire in queste tecnologie ed evolversi per supportarle: ne segue che questa rivoluzione tecnologica è inevitabile, la questione più importante è se la futura infrastruttura IoT verrà implementata in modo ideale, riuscendo a consentire l'economia collaborativa per la quale può garantire la massima efficienza, oppure se si formeranno anche in essa dei monopoli atti ad accentrare il controllo per favorire il profitto anche in quell'ambito. La gestione dell'economia della collaborazione e dello sfruttamento delle informazioni nello spazio di Internet è uno degli argomenti più importanti e attuali anche dal punto di vista legislativo[2].

## Internet delle comunicazioni, dell'energia e dei trasporti

L'obiettivo finale per raggiungere gli scopi descritti precedentemente consiste nella digitalizzazione e integrazione nell'infrastruttura di rete IoT dei dispositivi e dei processi in ogni ambito della catena del valore; l'infrastruttura unica dovrà comporsi dei tre cardini intorno a cui ruotano tutte le grandi economie mondiali e che sono stati la combinazione fondamentale per favorirne la crescita attraverso nuovi paradigmi nelle precedenti rivoluzioni industriali: le comunicazioni, l'energia e i trasporti[3]. Il primo insieme è quello più sviluppato, in quanto consiste proprio in Internet, che dagli anni '90 è cresciuto e si è evoluto fino a diventare la piattaforma di condivisione delle informazioni che tutti noi oggi conosciamo. Per garantire la sostenibilità di un'economia non più basata sulla scarsità ma capace di generare valore attraverso le relazioni tra le persone e i dispositivi in un'unica rete globale è necessario e fondamentale sfruttare le energie rinnovabili e condivisibili, che possono essere gestite appieno attraverso un'infrastruttura distribuita basata su IoT; lo stesso discorso vale per i trasporti e la logistica, altra caratteristica fondamentale su cui una società si deve basare per garantire la distribuzione fisica dei beni.

Di seguito vengono elencati alcuni degli esempi più importanti ad oggi osservabili in vari ambiti che mostrano come il nuovo paradigma dell'economia collaborativa stia portando evidenti miglioramenti per la qualità della vita nel suo complesso,

[2] https://www.startupbusiness.it/economia-della-condivisione-italia/88799/

[3]https://www.internet4things.it/mobile-wearable/la-digital-europe-di-rifkin-l-internet-of-things-trasforma-energia-trasporti-e-comunicazioni/

permettendo inoltre ai consumatori di diventare a loro volta produttori dei propri beni e servizi.

### *Energie rinnovabili*

Sempre più persone stanno diventando produttori della loro stessa energia, trasformando le loro case e imprese tramite l'utilizzo di energie rinnovabili e disponibili gratuitamente come energia solare, eolica, geotermica, idroelettrica e biomasse. Oltre ad avere un costo di raccolta tendente a zero, al contrario di combustibili fossili ed energia nucleare, che si basano su risorse limitate e difficili da estrarre, queste energie possono essere inoltre rivendute e ridistribuite e sono quindi capaci di ripagare i costi iniziali per gli impianti di raccolta, come pannelli solari e turbine eoliche. Il compito di gestione e distribuzione sarà affidato all'infrastruttura intelligente IoT che renderà possibile lo scambio reciproco in una rete globale dell'energia, similmente a come succede oggi con i contenuti informatici, e una gestione dei costi dinamica e dipendente dalla situazione, il tutto con prezzi di molto inferiori rispetto a quelli dettati dalle compagnie elettriche, basate su sistemi ancora fortemente centralizzati e poco adattabili alle oscillazioni di fabbisogno energetico.

La tendenza a questo approccio è recentemente sempre più favorita grazie ai miglioramenti esponenziali dei dispositivi nella capacità di catturare energia, a parità di prezzo; inoltre, in modo simile a quanto accadde con Internet per quanto riguarda le comunicazioni, i costi iniziali per l'installazione degli impianti verranno col tempo recuperati grazie alla natura a costo marginale zero dell'energia prodotta. Anche in questo ambito, lo sviluppo tecnologico crescente in modo esponenziale sta rendendo queste attività sempre più fattibili, fino al raggiungimento di un punto in cui ogni consumatore potrà diventare produttore della propria energia.

### *Stampa 3D*

L'utilizzo di stampanti 3D è il modello di produzione manifatturiera che si sta evolvendo insieme all'infrastruttura IoT ed è uno degli esempi più concreti attualmente osservabili associabili all'economia collaborativa. Il progresso tecnologico in questo campo ha già reso possibile a milioni di consumatori di aggirare i costi tipici riguardanti la produzione di beni, permettendo potenzialmente a chiunque di diventare produttore autonomo di una sempre più

crescente varietà di oggetti. La caratteristica fondamentale che ha dato un notevole vantaggio all'impresa per la stampa 3D rispetto alle classiche imprese manifatturiere, oltre al progressivo calo di prezzo delle stampanti che si sta verificando, è il carattere principalmente *open source* su cui si basa: sin dall'inizio le imprese basate su questo modello di produzione hanno incentivato fortemente la nascita di software open source sia per la gestione delle stampanti che per la produzione di oggetti. Esistono siti web dove vengono proposti modelli 3D appositi per la stampa che sono esenti da proprietà intellettuale, apposta per favorire l'implementazione di questa tecnologia su larga scala e la partecipazione e collaborazione all'interno delle community dedicate[4]. Oltre alla presenza di svariati modelli esenti da dispendiosi brevetti, un'altra caratteristica che permette di risparmiare sui costi è la natura intrinseca del processo di stampa, che procede per addizione invece che per sottrazione come avviene nelle fabbriche manifatturiere tradizionali: in questo modo viene risparmiata una notevole quantità di materia prima senza generare scarti. Inoltre, la digitalizzazione della produzione di beni attraverso software appositi favorisce la creatività e un alto grado di personalizzazione degli oggetti creati, il tutto sempre con costi più contenuti, e la natura distribuita della rete rende possibile connettersi e partecipare al processo di produzione e condivisione da qualunque posto, in opposizione alla classica produzione in serie centralizzata nelle fabbriche, penalizzata da elevati costi di gestione e di trasporto.

Questi sono i principali motivi che fanno della stampa 3D un fenomeno che è destinato senza dubbio a crescere nei prossimi anni, dove i costi sempre più bassi dei prodotti tecnologici permetteranno ai consumatori di diventare sempre più autonomi, traendo valore dalla partecipazione e collaborazione in una rete di scambio globale e distribuita che rispecchia tutti principi su cui si basa l'economia collaborativa, inclusa l'autonomia dalle classiche infrastrutture di produzione centralizzate e il conseguente risparmio dal punto di vista ecologico.

## *Istruzione online*

Il processo educativo centralizzato è sicuramente destinato, almeno in parte, a grandi cambiamenti nel futuro prossimo, vista la rapidità e facilità con cui è possibile condividere contenuti multimediali nell'Internet delle comunicazioni. Negli ultimi anni si è vista la crescita di corsi online finalizzati al conseguimento di crediti scolastici (*Massive Open Online Courses, MOOC*)[5], e la motivazione è

[4] https://www.thingiverse.com/

[5] http://www.scuola24.ilsole24ore.com/art/universita-e-ricerca/2018-06-15/boom-corsi-online-universita-fiutano-business-mooc-180046.php?uuid=AESgp76E

logica: in un mondo dove è possibile condividere informazioni a costi irrisori, un'aula virtuale formata da milioni di studenti costituisce, per certi versi, un'opportunità di apprendimento da non sottovalutare. La possibilità di seguire in ogni momento lezioni caricate su Internet da professori qualificati e di poter far parte di gruppi di studio virtuali in cui si possono condividere istantaneamente idee e appunti e trarre valore dalla collaborazione tra studenti nella stessa situazione è in ogni senso un potenziamento della scuola tradizionale.

Sempre più scuole e università stanno seguendo questo approccio, non solo a scopo pubblicitario per attirare studenti, ma anche perché rispecchia i valori che sono sempre stati propri dell'istruzione, concepita per essere libera e accessibile a tutti. Questo è l'ennesimo esempio di implementazione dei valori di partecipazione e collaborazione implementati sul già fortemente sviluppato Internet delle comunicazioni ed è indicativo della svolta che si sta prendendo a favore dell'azzeramento dei costi marginali dei servizi e a sfavore del modello centralizzato che da sempre caratterizza la società moderna.

### *Automazione industriale*

L'industria è il settore che ha potuto beneficiare maggiormente nel breve periodo dalle nuove tecnologie informatiche, come l'infrastruttura IoT, i Big Data, l'intelligenza artificiale, le tecniche di analisi avanzata che da ciò derivano e la robotica. L'implementazione di questo nuovo paradigma ha come conseguenza la sostituzione di diverse categorie di lavoratori umani; questo può non essere visto come un beneficio nel breve periodo, ma lo sarà sicuramente nel lungo periodo. Il settore industriale manifatturiero non è il solo in cui si manifesta questa tendenza: come nelle fabbriche le tecnologie di automazione basate sulle moderne infrastrutture provocano il minore impiego di lavoratori, anche in tante altre aree dei servizi vengono implementate sempre più soluzioni basate sull'intelligenza artificiale, che grazie allo svolgimento delle tecniche di analisi avanzata precedentemente descritte producono informazioni utili basate principalmente sulla statistica e sul riconoscimento di pattern, rendendo quasi obsoleto e sicuramente meno necessario l'utilizzo di persone, anche negli ambiti che inizialmente venivano considerati intoccabili da questo punto di vista.

Segnali evidenti di questa tendenza si possono osservare notando il calo di impiego registrabile in diversi settori negli ultimi anni, associato ad una crescita costante della produttività[6]; è necessario però sottolineare che questo calo non riguarda tutte le categorie di lavoratori: con l'evoluzione delle tecnologie, le figure lavorative

[6] https://www.corrierecomunicazioni.it/industria-4-0/il-paradigma-industria-40-vale-500-miliardi-l-anno/

sono destinate ad evolversi di conseguenza. Ne segue che in futuro si vedrà una diminuzione di richieste per varie categorie di lavoratori, opposte ad un aumento per quanto riguarda, ad esempio, le figure dei tecnici atte alla progettazione e alla gestione di tali impianti, ma anche alla nascita di nuove professioni[7]. Dal punto di vista delle imprese la scelta di queste tecnologie a sfavore dell'impiego umano è quasi solo un beneficio ed è indicativa dell'enorme vantaggio che si può ottenere attraverso l'utilizzo delle nuove tecnologie sopra elencate, in cui l'infrastruttura IoT è un componente fondamentale: l'integrazione dei macchinari con le tecniche di analisi avanzata basata sulla rilevazione dei sensori e sul riconoscimento di pattern è una garanzia di aumento di efficienza generale ed è fondamentale per la completa automazione dei procedimenti, e ha anch'essa come effetto la diminuzione dei costi marginali legati alle precedenti infrastrutture.

[7]http://www.ilsole24ore.com/art/impresa-e-territori/2016-10-03/nuove-professioni-industria-40-063726.shtml

## Principali problematiche riguardanti IoT

Nonostante le enormi potenzialità che caratterizzano l'infrastruttura IoT teorizzata, non sono poche le questioni importanti riguardanti la sua gestione, che se trascurate potrebbero pregiudicarne, anche totalmente, l'implementazione su larga scala. È quindi necessario ragionare sulle principali problematiche di cui tenere conto, analizzando in particolare le linee guida e le regolamentazioni che negli ultimi anni sono state tra gli argomenti principalmente discussi in ambito legislativo in relazione alla tecnologia IoT.

### Privacy e sicurezza

Una delle problematiche principali da considerare consiste nella gestione della proprietà sui dati e sui flussi informativi da parte dei fornitori di tali servizi, che per motivi legati alla competizione potrebbero abusare del proprio controllo sull'infrastruttura per porsi in una posizione di eccessivo vantaggio atto a sfavorire la concorrenza e garantire il mantenimento del proprio monopolio; tutto questo si può interpretare come la necessità di regolare a fondo le questioni riguardanti la privacy di tutti i soggetti coinvolti nei processi IoT, ponendo al contempo dei limiti al controllo che i fornitori di servizi possono esercitare, per garantirne uno svolgimento corretto e nel rispetto delle libertà e del diritto alla privacy dei singoli individui. Il riconoscimento dei limiti da fissare per garantire tali tutele in un mondo fortemente connesso e allo stesso tempo altamente suscettibile di abuso delle informazioni per fini personali, così come garantire il diritto dei singoli a controllare l'utilizzo dei propri dati in un'epoca che si preannuncia orientata alla trasparenza, alla collaborazione e all'inclusività è una delle questioni più discusse e difficili da gestire sin dall'avvento di Internet, e oggi più che mai è motivo di dibattito e regolamentazione nel mondo legislativo. Oltre a ciò, l'altra questione importante che mette a rischio la fattibilità di uno sviluppo futuro basato su queste tecnologie riguarda la sicurezza dei sistemi IoT, che dovendo operare sia nel mondo virtuale che in quello fisico sono considerati un bersaglio vantaggioso per qualsiasi hacker intenzionato a danneggiare o controllare i dispositivi e l'infrastruttura su cui si basano, senza escludere l'ambiente esterno con cui interagiscono[8]. Oltretutto, vista la varietà dei fornitori e dei dispositivi presenti sul mercato, non tutti sono soggetti agli stessi standard e nei casi peggiori ci si potrebbe trovare davanti a sistemi datati o dalla sicurezza trascurata dal punto di

[8] https://www.csoonline.com/article/3244467/internet-of-things/2018-prediction-securing-iot-connected-devices-will-be-a-major-cybersecurity-challenge.html

vista della progettazione del sistema, che in caso di attacco hacker sarebbero potenzialmente capaci di pregiudicare anche la sicurezza della rete a cui sono connessi, oltre che il loro funzionamento[9].

Con l'obiettivo di fornire delle linee guida sulle quali basare i futuri sviluppi di piattaforme IoT, la Commissione Europea ha fissato un principio generale, nel 2013, dichiarando che la protezione di privacy e dati, così come la sicurezza informatica, devono costituire un corredo gratuito dei servizi IoT. In particolare, la sicurezza informatica dev'essere considerata come tutela delle informazioni nella loro riservatezza, integrità e disponibilità; deve inoltre essere intesa come un requisito fondamentale nella fornitura dei servizi IoT destinati all'industria, sia per garantire la sicurezza informatica dell'organizzazione stessa sia a beneficio dei cittadini. Le linee guida propongono anche l'introduzione di meccanismi atti a scongiurare ogni elaborazione indesiderata dei dati personali e a segnalare di volta in volta al singolo il loro trattamento, le sue finalità e l'identità del soggetto che lo esegue, oltre alla procedura con cui far valere i propri diritti; nello stesso tempo, chi processa dati è tenuto a rispettare i principi che ne disciplinano la protezione. Viene evidenziata la necessità di assicurare che le persone conservino il controllo dei propri dati personali e che i sistemi IoT offrano sufficiente trasparenza per permettere agli individui di esercitare in modo efficace il proprio diritto alla tutela dei dati personali[10].

[9] https://www.corrierecomunicazioni.it/cyber-security/cybersecurity-natale-boom-attacchi-iot-mobile/
[10] https://ec.europa.eu/digital-single-market/en/news/conclusions-internet-things-public-consultation

## Regolamento generale sulla protezione dei dati (GDPR)

Il regolamento generale sulla protezione dei dati (*General Data Protection Regulation, GDPR*), denominato ufficialmente *regolamento (UE) n. 2016/679* è il più recente regolamento europeo in atto in materia di trattamento dei dati personali, entrato in vigore il 25 maggio 2016 e divenuto applicabile il 25 maggio 2018[11]. Dalla sua entrata in vigore, il GDPR ha sostituito la direttiva sulla protezione dei dati (*Direttiva 95/46/CE*) e, in Italia, ha in parte modificato e abrogato le norme incompatibili del decreto sulla protezione dei dati personali precedentemente in vigore (*D. Lgs. n. 196/2003*)[12].

### *Classificazione dei dati personali*

Per analizzare il nuovo regolamento e i principali cambiamenti che ha apportato è necessario definire le differenti categorizzazioni dei dati e i vari termini legati al loro trattamento; in questo ambito viene fatta distinzione tra dati personali e *categorie particolari* di essi considerate di natura più sensibile (*Art. 9, GDPR*).

Un dato personale è una qualsiasi informazione concernente una persona fisica identificata o identificabile, anche indirettamente, oppure informazioni riguardanti una persona la cui identità è nota o può comunque essere accertata mediante informazioni supplementari. In questa definizione, con il termine *identificabile* ci si riferisce sia ad un'individuazione diretta che indiretta, quindi anche ottenuta tramite l'incrocio con dati supplementari; la persona può essere identificabile univocamente rispetto ad ogni altro soggetto, o anche all'interno di una categoria. Se l'individuazione richiederebbe tempi e costi proibitivi può non essere presa in considerazione, ma non è comunque necessario raggiungere un elevato livello di identificabilità perché il dato sia soggetto a tutela. Indipendentemente dai metodi di riconoscimento impiegati, i dati vengono tutelati allo stesso modo; ne segue che anche un'informazione isolata o apparentemente innocua ma utilizzabile insieme ad altre per ottenere un'identificazione viene considerata un dato personale. Inoltre, le informazioni adoperate per rintracciare i dispositivi o gli ambienti di esecuzione attraverso cui una persona naviga in rete, nonostante non facciano riferimento ad una persona fisica, sono considerati dati personali. Grazie a questo criterio di individuazione che contempla l'incrocio con altri dati, si assoggettano alla tutela anche informazioni come l'indirizzo IP di un dispositivo nella rete,

[11] https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en
[12] https://www.garanteprivacy.it/regolamentoue

l’account di un servizio online, i dati di geolocalizzazione o i cookie utilizzati nei browser.

Esistono inoltre categorie particolari di dati personali soggette a maggiori limitazioni nel trattamento: sono tutti i dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, oppure dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona. Il loro trattamento è considerato valido solo in determinati casi, ad esempio se è stato dato il consenso esplicito in riferimento a una o più finalità specifiche, oppure se il trattamento è necessario per assolvere particolari obblighi.

Nel regolamento si fa riferimento all’implementazione di tecniche di *anonimizzazione* e *pseudonimizzazione* dei dati; è quindi necessario fare distinzione tra dati anonimi e dati pseudonimi. I dati anonimi sono le informazioni non originariamente associabili ad uno specifico interessato; i dati anonimi e anche quelli anonimizzati, ovvero che sono stati privati di tutti gli elementi identificativi, non sono ritenuti dati personali e quindi non sono soggetti alle relative norme. I dati pseudonimi, invece, sono quelli in cui gli elementi identificativi sono stati sostituiti da elementi diversi atti a rendere estremamente difficoltoso il riconoscimento dell’interessato; ovviamente devono essere adottate misure di protezione per quanto riguarda possibili abusi delle modalità esistenti per decifrarli, ovvero per ricollegare il dato pseudonimo al dato personale. Potendo consentire l’individuazione, anche se indiretta, della persona tramite l’incrocio con altre informazioni, i dati pseudonimi sono soggetti a tutela, anche se in modo minore rispetto ai dati personali veri e propri, in quanto il rischio relativo all’eventuale abuso di dati pseudonimizzati in modo sicuro è generalmente considerato improbabile. In ogni caso, un titolare che utilizza dati pseudo-anonimi invece di evitare l’utilizzo di dati personali è tenuto a comunicare la logica e le motivazioni di tale scelta agli interessati.

## *Trattamento dei dati personali*

Quando nel regolamento si fa riferimento al trattamento si intende una qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali, che comprendono:

- **Raccolta**, o acquisizione, che rappresenta generalmente l’inizio del trattamento.
- **Registrazione**, ovvero la memorizzazione dei dati su un qualsiasi supporto.

- **Organizzazione**, che consiste nella classificazione dei dati secondo un metodo prescelto.
- **Consultazione**, intesa come mera lettura o visualizzazione dei dati personali.
- **Comunicazione mediante trasmissione**: consiste nel dare conoscenza a terzi dei dati; è un'attività molto delicata in quanto implica il loro trasferimento a soggetti diversi dall'interessato, dal titolare, dal rappresentante e dagli incaricati alla gestione.
- **Diffusione (o qualsiasi altra forma di messa a disposizione)**: dare conoscenza dei dati a soggetti indeterminati.
- **Strutturazione** dei dati secondo particolari schemi.
- **Conservazione** dei dati su un qualsiasi supporto.
- **Adattamento** dei dati.
- **Modifica** dei dati.
- **Estrazione** di dati da insiemi già memorizzati.
- **Uso**, ovvero un'attività generica di impiego dei dati.
- **Raffronto**, ovvero un'operazione di confronto tra dati.
- **Interconnessione** dei dati attraverso strumenti elettronici.
- **Limitazione** dei dati.
- **Cancellazione**, ovvero l'eliminazione dei dati tramite strumenti elettronici.
- **Distruzione**, intesa come eliminazione definitiva dei dati.

### *Principi fondamentali del trattamento*

Il GDPR stabilisce dei principi fondamentali riguardanti il trattamento dei dati personali (*Art. 5, GDPR*), che fanno da base all'intera normativa, e che comprendono:

- **Principio di liceità, correttezza e trasparenza**: I dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato.
- **Principio di limitazione della finalità**: I dati personali devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modi non incompatibili con tali finalità. Non vengono considerate finalità incompatibili ulteriori trattamenti dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.
- **Principio di minimizzazione dei dati**: I dati personali devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.

- **Principio di esattezza**: I dati personali devono essere esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati.
- **Principio di limitazione della conservazione**: I dati personali devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati. Possono essere conservati per periodi più lunghi se trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.
- **Principio di integrità e riservatezza**: I dati personali devono essere trattati in maniera da garantirne un'adeguata sicurezza, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.
- **Principio di responsabilizzazione (accountability)**: Il titolare del trattamento è competente per il rispetto dei principi precedenti e in grado di comprovarlo. Questo principio stabilisce che il titolare è tenuto a adottare dei comportamenti proattivi in grado di assicurare il rispetto del regolamento.

### *Consenso al trattamento*

Il consenso al trattamento dei dati personali è uno degli elementi che ne costituisce la base giuridica. Per fornire un'informativa a riguardo adeguata e comprensibile per l'utente, le linee guida del GDPR in materia di trasparenza suggeriscono un approccio stratificato (al contrario di come potrebbe essere, ad esempio, una presentazione di tutte le informazioni su una stessa pagina), in modo che l'utente possa godere di una lettura più facilitata[13]. Inoltre, i contenuti dell'informativa annessa sono elencati in modo tassativo negli articoli 13 e 14; in particolare, il titolare è sempre tenuto a comunicare l'identità e i dati di contatto di titolare e responsabile, i dati di contatto del responsabile della protezione dei dati (se presente), la base giuridica del trattamento, il suo interesse legittimo nel caso costituisca la base del trattamento, se trasferisce dati personali a paesi terzi e, nel caso, attraverso quali strumenti. Sempre per garantire un'adeguata trasparenza, il regolamento prevede anche ulteriori informazioni da fornire, in particolare il tempo di conservazione dei dati (o i criteri seguiti per stabilire tale periodo) e il diritto dell'interessato di presentare un reclamo all'autorità di controllo. Nel caso il trattamento comporti processi decisionali automatizzati, come ad esempio la

[13] http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

profilazione, deve esserne specificata la presenza, insieme ad un'indicazione della logica dietro tali processi e le relative conseguenze per l'interessato. Per essere considerato lecito, il consenso deve essere:

- **Libero**: La decisione riguardo al consenso deve essere la conseguenza di una scelta effettiva, non condizionata in alcun modo, ovvero non devono essere presenti, ad esempio, intimidazioni o conseguenze negative in caso di mancato consenso.
- **Specifico**, ovvero relativo alla finalità per la quale il trattamento è eseguito; nel caso della presenza di più finalità differenti devono essere richiesti più consensi separati.
- **Informato**: L'interessato deve essere in condizione di conoscere tutte le caratteristiche del trattamento, come i dati trattati, le modalità, le finalità, i diritti che può esercitare e le conseguenze del suo consenso; per questo scopo è fondamentale la presenza di un'informativa che rispetti la precedente descrizione e dotata di un linguaggio facilmente comprensibile.
- **Inequivocabile**: Non deve sussistere alcun dubbio riguardo al fatto che l'interessato abbia espresso il proprio consenso al trattamento.
- **Verificabile**: Il titolare deve essere in grado di dimostrare che un particolare consenso è stato fornito in relazione ad uno specifico trattamento.
- **Revocabile**: Deve essere garantita la revocabilità del consenso; in particolare la revocabilità dovrebbe essere tanto facile quanto lo sia dare il consenso.[14]

### *Diritti dell'interessato al trattamento*

L'interessato è una persona fisica identificata o identificabile a cui i dati personali trattati fanno riferimento e gode di un insieme di diritti che può esercitare, che comprendono:

- **Diritto di accesso**: L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano, e in tal caso di ottenere l'accesso ai dati personali e ad altre informazioni che comprendono, ad esempio: le finalità, le categorie di dati personali trattati, i destinatari o le categorie di destinatari oggetto della comunicazione, il tempo di conservazione dei dati (o i criteri per determinarlo) e l'esistenza di un processo decisionale automatizzato, annessa ad una descrizione della sua logica e delle conseguenze che ne possono derivare (*Art. 15, GDPR*).

[14] http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

- **Diritto alla cancellazione (diritto all'oblio)**: Il titolare ha il diritto di ottenere la cancellazione dei dati personali che lo riguardano, nel caso sussistano particolari motivi che comprendono, ad esempio: la mancata corrispondenza con la finalità per la quale è svolto il trattamento, la revoca del consenso fornito, o se i dati sono stati trattati illecitamente (*Art. 17, GDPR*).
- **Diritto di limitazione**: Per l'interessato è possibile richiedere la limitazione del trattamento in casi particolari tra cui sono presenti, ad esempio, le seguenti situazioni: se l'interessato ne contesta l'esattezza, se ne richiede la limitazione dell'utilizzo invece che richiederne la cancellazione in seguito ad un utilizzo illecito, o se sono necessari per l'accertamento, l'esercizio o la difesa di un proprio diritto in sede giudiziaria (*Art. 18, GDPR*).
- **Diritto alla portabilità**: L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare senza impedimenti da parte del titolare del trattamento cui li ha forniti, nelle situazioni in cui il trattamento sia effettuato con mezzi automatizzati e sia basato sul consenso o su un contratto. Questo viene spesso finalizzato attraverso la messa a disposizione da parte del titolare di un servizio per ottenere automaticamente i propri dati oggetto di trattamento, e garantendo una trasmissione diretta dei dati ad un altro titolare, se tecnicamente fattibile (*Art. 20, GDPR*).[15]

### *Titolare, responsabile del trattamento e DPO*

Il titolare del trattamento (*data controller*) è colui che determina le finalità, le modalità e gli strumenti utilizzati nell'ambito del trattamento di dati personali, comprese le decisioni riguardanti la sicurezza; può essere una persona fisica, giuridica, la pubblica amministrazione o qualsiasi altro ente, organismo o associazione cui competono tali decisioni. È una figura distinta da chi gestisce i dati, che si occupa in particolare di stabilire i motivi e i modi del trattamento ed è responsabile giuridicamente dell'ottemperanza degli obblighi previsti dalla normativa; è anche colui che deve mettere in atto le misure di sicurezza atte a garantire il rispetto dei diritti dell'interessato. È suo compito nominare il responsabile del trattamento attraverso un contratto o un atto giuridicamente valido.

Il responsabile del trattamento (*data processor*), invece, è la persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati per conto del titolare.

[15] http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233

Deve fornire garanzie per assicurare il rispetto della normativa e dei diritti degli interessati e deve essere dotato delle competenze adeguate a farlo, ovvero una conoscenza specialistica della materia, oltre che disporre degli strumenti adeguati a mettere in atto tali procedimenti.

Una delle principali modifiche alla precedente normativa introdotte dal GDPR è l'aggiunta, oltre alle classiche figure di titolare e responsabile, di quella del responsabile della protezione dei dati personali (*Data Protection Officer, DPO*), nominato, ad esempio, nei casi in cui venga effettuato un monitoraggio dei dati degli interessati su larga scala, in modo sistematico e regolare, nel caso vengano trattate le categorie particolari di dati personali su larga scala, oppure se il trattamento è svolto da un'autorità o organismo pubblico (*Art. 37, GDPR*). Il responsabile della protezione dei dati personali deve disporre delle adeguate conoscenze in materia di protezione dei dati e svolge funzioni di consulenza, supporto e controllo a riguardo; funge inoltre da punto di contatto tra le figure di vigilanza interna all'azienda (titolare e responsabile che lo nominano) e l'autorità di controllo, con la quale collabora (*Artt. 38 e 39, GDPR*).[16]

### *Principi di privacy by design e by default*

Tra gli obblighi del titolare vi è quello di garantire l'attuazione delle misure di sicurezza tenendo conto dello stato dell'arte, dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, contemplando anche i rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento. In questo ambito il GDPR indica alcune misure di sicurezza da implementare e stabilisce dei principi da rispettare, imponendo l'obbligo alle aziende di sviluppare un progetto tenendo conto fin da subito degli strumenti a tutela dei dati personali. I principi da rispettare secondo la normativa comprendono:

- **Privacy by design (privacy sin dalla progettazione)**: È necessario valutare sin dall'inizio eventuali problemi, in modo da non pregiudicare le attività di progettazione successive; il focus deve essere sulla prevenzione delle situazioni che si possono verificare invece che su un'eventuale correzione successiva. È un approccio basato sulla valutazione del rischio, dove si considerano le problematiche che si possono presentare prima che il trattamento inizi; è dipendente dalla tecnologia, perciò è suscettibile di adattamenti nel corso del tempo.

[16] http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048

- **Privacy by default (privacy come impostazione predefinita)**: Stabilisce che le imprese dovrebbero gestire i dati personali considerando il trattamento dei soli dati necessari e sufficienti alle finalità prefissate e per il solo periodo strettamente necessario. Queste misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica (*Art. 25, GDPR*).

### *Valutazione di impatto del trattamento*

Il nuovo regolamento propone un approccio basato sulla valutazione di impatto del trattamento (*Data Protection Impact Assessment, DPIA*), che è un onere posto a carico del titolare, il quale deve effettuare una valutazione del rischio che può conseguire a seguito dell'implementazione delle tecniche di trattamento presenti nel progetto, dove il rischio è relativo alle libertà e ai diritti delle persone fisiche, come ad esempio eventuale danno fisico, materiale o immateriale, discriminazione, furto d'identità, perdite finanziarie, pregiudizio alla reputazione, decifratura non autorizzata della pseudonimizzazione o un qualsiasi altro danno significativo di natura sociale o economica.

In questa fase è particolarmente efficace la presenza del responsabile della protezione dei dati, con il quale il titolare si consulta a riguardo nel caso ne sia stato designato uno, e che con la sua supervisione si assicura che la valutazione venga fatta nel rispetto del regolamento e dei suoi principi. La valutazione d'impatto è richiesta in particolare nei seguenti casi:

- Nel caso venga effettuata una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche.
- Nel caso venga effettuato un trattamento su larga scala delle *categorie particolari* di dati personali, o di dati relativi a condanne penali o reati.
- Nel caso di sorveglianza sistematica e su larga scala di una zona accessibile al pubblico.

La valutazione deve contenere, almeno:

- Una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento.

- Una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità.
- Una valutazione dei rischi per i diritti e le libertà degli interessati.
- Le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al regolamento (*Art. 35, GDPR*).

Il vantaggio di un approccio basato sul rischio è fondamentalmente quello di richiedere l'adempimento di obblighi che possono andare oltre quelli richiesti dalla legge. È inoltre più flessibile e adattabile in base agli strumenti tecnologici utilizzati e agli scopi dello specifico progetto in questione e tiene conto delle specifiche esigenze dell'azienda.[17][18]

## GDPR in ambito IoT

Vista la natura dei sistemi IoT e la loro implementazione su larga scala, i soggetti che accedono ai dati sono potenzialmente un numero incalcolabile, determinando di conseguenza elevati rischi relativi alla gestione di eventuali dati personali. È quindi fondamentale identificare le figure di titolare, responsabile, DPO ed eventuali incaricati e far fronte ai rischi principali che caratterizzano queste tecnologie, che possono comprendere:

- Furto ed uso illecito dei dati acquisiti.
- Hackeraggio di sistemi IoT con lo scopo di alterare e manipolare i dati gestiti.
- Hackeraggio di sistemi IoT con lo scopo di manipolarne il funzionamento, capace di causare danni anche fisici alle persone presenti nell'ambiente esterno con cui interagiscono.

I principi da rispettare durante la progettazione dei sistemi IoT nell'ambito del GDPR corrispondono a quelli precedentemente descritti per del ciclo di vita dei sistemi che trattano dati personali, con particolare enfasi per quanto riguarda l'implementazione delle tecniche di privacy by design. Ciò significa che il progettista dovrà valutare sin da subito i rischi derivanti dall'interconnessione del dispositivo con gli altri nella rete, facendo particolare attenzione alla minimizzazione dei dati trattati, e tenere d'occhio l'evoluzione del sistema in relazione allo stato attuale della tecnologia, modificandolo di conseguenza anche per ovviare alle problematiche di sicurezza che altrimenti ne deriverebbero. È necessario effettuare anche la valutazione di impatto del trattamento, se si ritiene

[17] https://www.garanteprivacy.it/regolamentoue/DPIA
[18] http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

che possa presentare rischi elevati, o nei casi descritti precedentemente in cui risulti obbligatoria.

Essendo fortemente correlata all'uso di IoT o di Big Data (o in sistemi che integrano entrambe le tecnologie, dovendo fare uso di enormi moli di dati per i propri scopi), nonché citata più volte nel regolamento, in particolare per quanto riguarda situazioni che possono presentare un rischio elevato e correlata ai meccanismi di decisioni automatizzate, è bene dare la definizione di *profilazione*. Per profilazione si intende l'insieme delle attività di raccolta ed elaborazione di dati svolte sugli utenti di un servizio, per effettuarne una suddivisione in categorie; è definita come un procedimento automatizzato volto a valutare aspetti personali (e che quindi opera su dati personali) riguardanti una persona fisica. Gli scopi principali consistono nel valutare attraverso analisi o previsioni aspetti come il comportamento, le preferenze, gli interessi, gli spostamenti o l'affidabilità di una persona, o nel prendere decisioni sulla base di essi; uno dei settori in cui viene adoperata più spesso è, ad esempio, quello del marketing informatico per l'invio di pubblicità basata sul comportamento degli utenti. Le linee guida a riguardo sottolineano l'importanza di perseguire il principio di trasparenza nella comunicazione della logica su cui si basa la profilazione: essendo spesso un procedimento invisibile all'interessato e che si basa su algoritmi complessi per derivare dati generati sulla base dei dati personali, risulta spesso difficile da capire; per questo si vede la necessità di fornire informazioni coincise, facilmente accessibili e di più facile comprensione possibile[19].

## Proprietà dei dati

Per quanto riguarda il possesso dei dati che vengono utilizzati dai dispositivi, la proprietà appartiene di fatto alle imprese che li possiedono e che forniscono i servizi che ne elaborano le informazioni, che spesso si adoperano per assicurarselo attraverso un contratto incluso con l'acquisto del prodotto. Questa tuttavia potrebbe non essere la scelta più efficiente, siccome seguendo un approccio orientato alla trasparenza il concetto di proprietà stesso non dovrebbe essere considerato un problema per i limiti che possono essere posti ai fruitori di tali servizi.

È anche da notare che, oltre ad essere naturalmente interessate a mantenere il possesso dei dati generati dai propri sistemi, le imprese sono ancora più interessate a poter definire gli standard che regolano la loro gestione all'interno della rete; infatti, visto che il valore dei dati è dato dalla capacità di elaborarli ed aggregarli

[19] http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

per trarne relazioni utili, l'accesso ad essi assume in questo contesto un significato molto più importante del possesso, nonostante anch'esso costituisca un vantaggio fondamentale. Per questo motivo è necessario focalizzarsi sulla condivisione più che sull'esclusione, garantendo a tutti i soggetti che interessano un processo IoT il dovuto accesso ai dati, fornendogli le viste adeguate a svolgere i loro compiti per permettere a chiunque li adoperi di non essere ingiustamente limitato nello svolgimento delle proprie funzioni. Normalmente, garantire un controllo del genere non sarebbe negli interessi di chi li possiede, ma va ricordato che tutto ciò è necessario e fondamentale per il corretto funzionamento dei cosiddetti sistemi di sistemi, che si basano proprio sulla condivisione per migliorare l'efficienza di ognuno, scambiandosi dati sul proprio funzionamento, ed è anche il principio su cui si dovrebbe basare l'implementazione di tali sistemi precedentemente ipotizzata.

Tra i soggetti a cui va garantito un controllo adeguato vi sono le imprese che producono i dispositivi, che devono contemplare l'integrazione in sistemi più grandi e che quindi devono sottoporre il loro flusso di dati alla gestione delle imprese proprietarie dei sistemi più popolari sul mercato a cui gli altri dispositivi devono potersi obbligatoriamente adattare, questo anche per favorire una competizione equa. Questo discorso si può estendere anche ai consumatori: ciò che rende interessanti i dispositivi IoT moderni è proprio la capacità di poter controllare le informazioni che elaborano; di conseguenza, privare gli utenti di questa autonomia nella loro gestione andrebbe contro il motivo per cui sono stati intesi in primo luogo, penalizzando sia loro che le imprese, in quanto si porrebbe una limitazione alla loro capacità di fornire le funzionalità ormai considerate fondamentali e tipiche dei prodotti IoT, e ultimamente favorendo ogni concorrenza che deciderà invece di continuare a farlo.

Il dibattito più acceso sul possesso riguarda però l'utilizzo che può essere fatto dei dati da parte di chi ne ha l'effettiva proprietà, che visto il loro enorme potenziale potrebbe fornirli a sua volta a terzi per permettergli di derivarne altre informazioni utili ai loro scopi, come può essere ad esempio nel caso di un servizio di pubblicità comportamentale basato sui dati raccolti sugli utenti. Il GDPR è stato concepito anche per rafforzare la tutela degli interessati per quanto riguarda queste transazioni, garantendo la possibilità di conoscere le motivazioni riguardanti gli utilizzi che verranno fatti delle informazioni, fornendo gli strumenti per sapere quali dati vengono trattati e un'identificazione chiara delle varie figure addette alla loro gestione, con l'ulteriore effetto di sensibilizzare le persone riguardo le enormi potenzialità e problematiche derivanti dal loro sfruttamento.

# Conclusione

L'implementazione di un'architettura basata su uno standard aperto e condiviso sarà necessaria per venire incontro fin da subito ai problemi di sicurezza e di rispetto della privacy che tendono a scoraggiare chiunque si voglia affidare alle nuove tecnologie IoT, nonché fondamentale per evitare il formarsi di monopoli difesi dalla proprietà intellettuale.

La cosa certa è che la caratteristica di azzerare i costi dei procedimenti digitalizzati, resa possibile dall'integrazione di queste tecnologie lungo tutta la catena del valore, ha innescato una trasformazione che è destinata a modificare sostanzialmente i classici modelli economici: la disponibilità di informazioni dettagliate e in tempo reale sui prodotti e sui processi sta cambiando il modo in cui si crea valore, quello in cui le imprese competono e la loro relazione con i consumatori. È un cambiamento che influenzerà, direttamente o indirettamente, ogni impresa, che si vedrà costretta a ridefinire i ruoli relativi al settore informatico integrandoli in molti altri, mentre altre compagnie diventeranno esclusivamente produttrici di software, vista la sua crescente priorità rispetto all'hardware: la produzione è destinata, in un certo senso, a far parte di ogni momento del ciclo di vita dei prodotti, che potranno essere costantemente monitorati e aggiornati di conseguenza, fornendo un servizio di evoluzione continuo, orientato alla durabilità e basato sulle abitudini e sulle esigenze degli utenti.

Si stanno inoltre diffondendo nuovi modelli di business, come quello di *product-as-a-service*, in cui un prodotto viene pagato in base all'utilizzo che ne viene fatto, con l'assenza di costi fissi. In questo modo il produttore scambia la sua capacità di fornire un servizio efficiente e continuo in cambio del mantenimento della gestione: il dispositivo diventa quindi un mezzo attraverso il quale si può dare accesso alle soluzioni pensate per il cliente tramite gli innovativi metodi di analisi dei dati e per questo motivo destinato a durare più a lungo. Sulla stessa linea si sta diffondendo anche il modello di *product-sharing*, che si basa sulla condivisione di beni che vengono utilizzati in modo intermittente, garantendo una soddisfazione sia per il consumatore grazie al risparmio e alla minore necessità di acquistarne di nuovi, sia per le imprese, che hanno a disposizione nuovi campi in cui evolversi per gestire tutti questi nuovi servizi di carattere puramente informatico.

Queste nuove tendenze sono indicative di come la nuova rivoluzione tecnologica stia indirizzando il paradigma verso quello di un'economia collaborativa, basata sulla partecipazione di persone e oggetti in una rete globale con il fine di creare valore digitale attraverso nuovi servizi e di promuovere conseguentemente il risparmio e il riuso dei beni, facendo affidamento su fonti di energia rinnovabile e basandosi sulla condivisione e sulla trasparenza, ponendo al contempo il

consumatore in una situazione di controllo e di autonomia fino a pochi decenni fa considerata inconcepibile e fornendo possibilità inedite per generare profitto in modo sostenibile.

## Bibliografia


*2018 reform of EU data protection rules.* (2018). Tratto da Sito Web Commissione Europea: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

Ashton, K. (2009, 6 22). *That 'Internet of Things' Thing.* Tratto da RFID Journal: http://www.rfidjournal.com/articles/view?4986

*Big Data - Wikipedia.* (s.d.). Tratto da Wikipedia: https://en.wikipedia.org/wiki/Big_data

Biscella, M. (2016, 10 3). *Nuove professioni da Industria 4.0.* Tratto da Il Sole 24 Ore: http://www.ilsole24ore.com/art/impresa-e-territori/2016-10-03/nuove-professioni-industria-40-063726.shtml

Bruno, E. (2018, 6 18). *Boom dei corsi online: le università fiutano il business dei Mooc.* Tratto da Il Sole 24 Ore: http://www.scuola24.ilsole24ore.com/art/universita-e-ricerca/2018-06-15/boom-corsi-online-universita-fiutano-business-mooc-180046.php?uuid=AESgp76E

*Conclusions of the Internet of Things public consultation.* (2013, 2 28). Tratto da Sito Web Commissione Europea: https://ec.europa.eu/digital-single-market/en/news/conclusions-internet-things-public-consultation

Curreli, E., & Bellezza, M. (2016, 10 8). *Economia della condivisione, i punti cardine della proposta di legge italiana.* Tratto da Startupbusiness: https://www.startupbusiness.it/economia-della-condivisione-italia/88799/

DeLoach, D., Berthelsen, E., & Elrifai, W. (2017). *The Future of IoT: Leveraging the shift to a data centric world.*

*Edge Computing - Wikipedia.* (s.d.). Tratto da Wikipedia: https://en.wikipedia.org/wiki/Edge_computing

Frollà, A. (2017, 5 15). *Il "paradigma" Industria 4.0 vale 500 miliardi.* Tratto da CorCom: https://www.corrierecomunicazioni.it/industria-4-0/il-paradigma-industria-40-vale-500-miliardi-l-anno/

*Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation.* (2018). Tratto da Sito Web Commissione Europea: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

*Guidelines on Consent under Regulation.* (2018). Tratto da Sito Web Commissione Europea: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

*Guidelines on Data Protection Impact Assessment.* (2018). Tratto da Sito Web Commissione Europea: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

*Guidelines on Data Protection Officers ('DPOs').* (2018). Tratto da Sito Web Commissione Europea: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048

*Guidelines on the right to "data portability".* (2018). Tratto da Sito Web Commissione Europea: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233

*Guidelines on Transparency under Regulation.* (2018). Tratto da Sito Web Commissione Europea: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

*Internet of Things - Wikipedia.* (s.d.). Tratto da Wikipedia: https://en.wikipedia.org/wiki/Internet_of_things

Krceva, K. (2015, 5 28). *La "Digital Europe" di Rifkin: l'Internet of Things trasforma energia, trasporti e comunicazioni.* Tratto da Internet4Things: https://www.internet4things.it/mobile-wearable/la-digital-europe-di-rifkin-l-internet-of-things-trasforma-energia-trasporti-e-comunicazioni/

*Machine to Machine - Wikipedia.* (s.d.). Tratto da Wikipedia: https://en.wikipedia.org/wiki/Machine_to_machine

MakerBot Industries, LLC. (s.d.). *Thingiverse - Digital Designs for Physical Objects*. Tratto da Thingiverse: https://www.thingiverse.com/

Persaud, N. (2017, 12 22). *2018 prediction: securing IoT-connected devices will be a major cybersecurity challenge.* Tratto da CSO Online: https://www.csoonline.com/article/3244467/internet-of-things/2018-prediction-securing-iot-connected-devices-will-be-a-major-cybersecurity-challenge.html

Porter, M. E., & Heppelmann, J. E. (2014). How Smart, Connected Products Are Transforming Competition. *Harvard Business Review*.

Porter, M. E., & Heppelmann, J. E. (2015). How Smart, Connected Products Are Transforming Companies. *Harvard Business Review*.

*Regolamento europeo in materia di protezione dei dati personali - Pagina informativa.* (2018). Tratto da Sito Web Garante Privacy: https://www.garanteprivacy.it/regolamentoue

Rifkin, J. (2017). *La società a costo marginale zero. L'internet delle cose, l'ascesa del «Commons» collaborativo e l'eclissi del capitalismo.* Milano: Mondadori.

Salerno, A. (2017, 11 29). *Cybersecurity, a Natale boom di attacchi contro IoT e mobile.* Tratto da CorCom: https://www.corrierecomunicazioni.it/cyber-security/cybersecurity-natale-boom-attacchi-iot-mobile/