Consiglio Nazionale delle Ricerche
Istituto di Calcolo e Reti ad Alte Prestazioni

Analisi del contesto di riferimento normativo nazionale ed internazionale applicabile ai dispositivi IoT

Danilo Cistaro, Rosaria De Simone, Agostino Forestiero

RT- ICAR-CS-23-10 **Dicembre 2023**

Consiglio Nazionale delle Ricerche, Istituto di Calcolo e Reti ad Alte Prestazioni (ICAR)
– Sede di Cosenza, Via P. Bucci 8-9C, 87036 Rende, Italy, URL: *www.icar.cnr.it*
– Sezione di Napoli, Via P. Castellino 111, 80131 Napoli, URL: *www.icar.cnr.it*
– Sezione di Palermo, Via Ugo La Malfa, 153, 90146 Palermo, URL: *www.icar.cnr.it*

SOMMARIO

INTERNET OF THINGS

L'Internet of Things (IoT) rappresenta una rivoluzione nella connessione e nell'interazione tra dispositivi fisici e l'ambiente digitale. Si tratta di una rete di oggetti connessi tra loro e al mondo online, capaci di raccogliere e scambiare dati attraverso sensori, software e altre tecnologie, consentendo una vasta gamma di applicazioni in settori diversi come la casa intelligente, la salute, l'industria, l'agricoltura, la mobilità e molti altri.

L'IoT ha già avuto un impatto significativo sul modo in cui viviamo e lavoriamo, facilitando la creazione di ambienti più efficienti, sicuri e connessi. Tuttavia, il suo futuro promette di essere ancora più rivoluzionario. Le previsioni indicano una crescita esponenziale del numero di dispositivi connessi, con una previsione di decine di miliardi di oggetti entro i prossimi anni.

Tra le tendenze future dell'IoT ci sono l'evoluzione delle reti di comunicazione, come la transizione verso reti 5G, che forniranno connettività più veloce, affidabile e di latenza ultra-bassa, consentendo un maggiore sviluppo di applicazioni IoT avanzate. Inoltre, l'intelligenza artificiale e il machine learning continueranno a giocare un ruolo cruciale nell'analisi dei dati generati dagli oggetti connessi, consentendo un'elaborazione più sofisticata e in tempo reale per fornire insights più approfonditi e azioni predittive.

L'IoT continuerà a influenzare settori come la sanità, l'agricoltura, la mobilità urbana e l'industria, migliorando l'efficienza operativa, ottimizzando le risorse e creando nuove opportunità di business. Tuttavia, saranno fondamentali una sicurezza informatica robusta e regolamentazioni adeguate ad affrontare le sfide legate alla privacy e alla protezione dei dati in un mondo sempre più connesso.

Ciononostante, la maggior parte delle volte, i progettisti di sistemi IoT non danno sufficiente considerazione all'aspetto più importante dell'IoT, che riguarda principalmente la sicurezza e la privacy.

La sicurezza di un sistema non riguarda solo i problemi tecnici, ma è legata maggiormente alla consapevolezza della sicurezza tra i professionisti, alla mentalità e alla predisposizione delle persone o delle organizzazioni a questo approccio, nonché ai processi coinvolti. La sicurezza e la privacy dei dati sono aspetti molto importanti nella progettazione e nella distribuzione dei dispositivi IoT.

La rapida crescita del numero di dispositivi connessi, la vasta eterogeneità dei dispositivi, le risorse limitate, la privacy, gli aggiornamenti software e l'ambiente operativo creano importanti sfide che sono legate alla sicurezza in questo settore.

Ognuna delle caratteristiche presenta i suoi aspetti progettuali che devono essere considerati dai progettisti IoT per implementare un sistema IoT più sicuro, sicurezza che andrà a beneficio dei consumatori finali dei prodotti IoT, che potrebbero finalmente acquistare il dispositivo IoT preferito ma che a questo punto è stato sviluppato utilizzando strumenti e processi sicuri e che inoltre preserva la propria privacy. Ciononostante, è ugualmente difficile affrontare queste sfide anche avendo alle spalle una base consistente di lavoro che è stato condotto per decenni nel settore della sicurezza e della privacy.

o LE ORIGINI DEL CONCETTO DI PRIVACY E LA SUA EVOLUZIONE

Il termine inglese privacy è traducibile con riservatezza, è il diritto alla riservatezza delle informazioni personali e della propria vita privata: *the right to be let alone* (“il diritto di essere lasciati in pace”), secondo la formulazione del giurista statunitense Louis Brandeis che fu probabilmente il primo al mondo a formulare una legge sulla riservatezza.

In realtà, per privacy si intende comunemente il diritto della persona di impedire che le informazioni che la riguardano vengano trattate da altri, a meno che il soggetto non abbia volontariamente prestato il proprio consenso.

L'attuale nozione di *privacy* è frutto di una lunga evoluzione concettuale che, negli anni, ha arricchito di implicazioni e significati un'idea particolarmente complessa, dinamica ed in continuo mutamento.

Dopo una lunga fase di sviluppo, il diritto alla *privacy* tende oggi ad assumere nuovi significati in virtù del diverso contesto culturale, sociale, economico e tecnologico che caratterizza l'odierna società dell'informazione.

L'espressione "*diritto alla privacy*" rientra pienamente nel linguaggio di uso comune dell'odierna società dell'informazione, ma le sue origini sono alquanto remote. Il concetto inizia a delinearsi già ai tempi dell'Antica Grecia, quando si riscontra per la prima volta il senso di riservatezza in alcuni trattati filosofici di notevole rilievo. Per gli antichi greci la partecipazione alla vita pubblica da parte dei propri cittadini maschi era considerata fondamentale e per certi versi, un vero e proprio dovere da adempiere; analogamente, riconoscevano ad ogni uomo la necessità di possedere una sfera privata e riservata, intesa come un ambiente destinato ad assolvere unicamente ai bisogni e alle esigenze personali.

Durante il medioevo, e in modo particolare durante l'età feudale, il termine privato diviene gradualmente sinonimo di "familiare", assumendo il significato di ciò che si trova in disparte, ciò che è segreto, nascosto, riservato, ovvero ciò che non è "pubblico". Inizia così ad affermarsi la sfera del privato.

Eppure, il concetto di *privacy* inteso nella forma a noi più vicina, si afferma con il disgregarsi della società feudale, in cui esisteva una fitta rete di relazioni tra gli individui che si riflettevano nel modo di organizzare la loro stessa vita quotidiana.

Bisognerà poi attendere fino al XVI secolo per modificare la mentalità, infatti, secondo lo storico medievale Ariès, tra il XVI e il XVIII secolo ci furono tre evoluzioni fondamentali che determinarono la trasformazione delle società occidentali: il nuovo ruolo ricoperto dallo Stato, lo sviluppo dell'alfabetizzazione e le riforme religiose. Questi tre elementi, connessi tra loro, modificarono profondamente i ruoli nella vita quotidiana della società medievale, contribuendo a diffondere uno stile di vita alternativo e a creare di conseguenza, un nuovo costume, che prima riservato all'uomo di corte e che poi si diffuse all'intera società.

Successivamente, un contributo essenziale lo diedero Samuel Warren e Louis Brandeis, due giuristi statunitensi che nel 1890 pubblicarono un saggio intitolato "*The Right of Privacy"*, noto in letteratura per essere considerato la prima monografia giuridica a riconoscere l'esistenza di un diritto autonomo alla *privacy*, meglio definito come "*the right to be let alone*", ossia il "diritto di essere lasciato solo".

Diversamente dal nome, l'idea che sta dietro il concetto espresso dal "the *right to be let alone*" non consiste nel desiderio della persona "ad essere lasciata sola", ma va inteso più che altro come il desiderio della persona non vedere violata la propria intimità e garantire la tranquillità della propria vita privata.

Il diritto alla *privacy*, ha subito una notevole espansione per quanto riguarda i contenuti; tale espansione è dovuta dalla necessità di far rientrare nel proprio ambito di tutela diverse situazioni soggettive emerse nel tempo con lo scopo di supportare i diversi contesti socio-culturali che sono stati determinati dagli sviluppi economici e tecnologici degli ultimi decenni.

Infatti, con l'introduzione dei primi strumenti tecnologici, è sorta la necessità di avere una specifica tutela riguardo il rapporto presente tra "riservatezza-computer"; l'impiego dei computer consente di impadronirsi di informazioni che riguardano l'individuo che possono essere archiviate, comprese quelle della vita privata.

Nel 2013 le rivelazioni di Edward Snowden hanno riposto al centro dell'attenzione mondiale l'importanza della protezione dei dati personali, sollevando la questione privacy all'interno dei maggiori dibattiti politici, sociali e giuridici di portata internazionale. Il caso Datagate ha svelato al mondo intero l'esistenza di una gigantesca "macchina della sorveglianza" manovrata dal governo USA e dall'NSA (National Security Agency) che, seppur giustificata da esigenze di sicurezza nazionale e di lotta al terrorismo, delinea il quadro di una società del controllo globale che mira in maniera decisamente intrusiva sia alla privacy dei cittadini che alla libertà degli Stati stessi.

Il caso Datagate mostra una realtà che sottolinea l'inadeguatezza della normativa vigente, nonché la necessità di attuare degli interventi più rigidi in materia di tutela della privacy.

Del diritto alla privacy si è sempre discusso sin dalla sua affermazione, ed è ammirevole come, a distanza di secoli, c'è chi ancora continua a battersi affinché esso non venga calpestato o messo in secondo piano dalle nuove leggi che dominano la società. Snowden ha sacrificato la propria vita rinunciando alla propria liberta per contrastare l'invadenza delle agenzie di sicurezza governative [1].

LA PRIVACY NELL'ERA DELL'INTERNET OF THINGS

Una delle problematiche principali da considerare nell'Internet of Things, consiste nella gestione della proprietà sui dati e sui flussi informativi da parte dei fornitori di servizi IoT, che per motivi legati alla competizione sul mercato potrebbero abusare del proprio controllo sull'infrastruttura per porsi in una posizione di netto vantaggio atto a sfavorire la concorrenza e garantire il mantenimento del proprio monopolio; tutto ciò può essere interpretato come la necessità di regolamentare fino in 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 nel pieno rispetto delle libertà e del diritto alla privacy dei singoli individui.

Una questione importante che mette a rischio la fattibilità dello 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 ottimo bersaglio da parte di qualsiasi hacker intenzionato a danneggiare o a controllare i dispositivi e l'infrastruttura su cui si basano, senza escludere l'ambiente esterno con cui interagiscono. Oltretutto, vista la varietà dei vendor e dei dispositivi presenti sul mercato, non tutti sono soggetti agli stessi standard e nei casi peggiori ci si potrebbe trovare difronte sistemi datati o dalla sicurezza trascurata dal punto di 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, come accaduto ad esempio con la botnet Mirai [2].

Nel 2013 la Commissione Europea, con l'obiettivo di fornire delle linee guida sulle quali basare i futuri sviluppi delle piattaforme IoT, ha fissato un principio generale dichiarando che la protezione della privacy e dei dati, così come la sicurezza informatica, devono costituire un corredo gratuito dei servizi IoT.

In particolare, la sicurezza informatica deve essere considerata come tutela delle informazioni nella loro riservatezza, integrità e disponibilità; deve inoltre essere intesa come requisito fondamentale nella fornitura dei servizi IoT destinati all'industria, sia per garantire la sicurezza informatica dell'organizzazione stessa sia per il 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; allo stesso tempo, chi processa dati è tenuto a rispettare i principi che ne disciplinano la protezione.

Viene sottolineata 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 [3].

Grazie alla diffusione degli smart devices a basso costo e all'uso diffuso delle reti wireless ad alta velocità si è ottenuto un rapido sviluppo dell'Internet of Things.

L'IoT, per come è stato definito, comprende diversi dispositivi fisici embedded con tag RFID (Radio Frequency Identification), ma anche sensori e attuatori. Tutti questi device consentono l'interazione e la cooperazione sia attraverso protocolli di comunicazione tradizionali sia attraverso protocolli IoT ed hanno la peculiarità di essere dei dispositivi pervasivi ed eterogenei che consentono di interagire sia con il mondo fisico sia con il mondo digitale, consentendo di migliorare significativamente la qualità della vita delle persone che interagiscono con l'IoT, fornendo loro una vasta gamma di applicazioni e servizi.

Molti servizi nell'IoT richiedono l'apprendimento di quelli che sono gli interessi e le preferenze degli utenti mediante un'analisi completa dei dati raccolti attraverso un gran numero di dispositivi fisici che mettono in discussione la privacy delle informazioni personali e lo sviluppo dell'IoT.

A questo punto inizia ad emergere un particolare problema inerente alla privacy, in cui si evince una netta separazione tra gli utilizzatori che sono propensi all'utilizzo dei servizi IoT, in quanto molti individui sono favorevoli ai benefici introdotti dall'impiego di tali servizi, ed altri che invece temono che i propri dati personali possano essere condivisi.

In un sondaggio che ha condotto IEEE e che riguarda l'IoT, il 46% degli utilizzatori di servizi per l'IoT considera le preoccupazioni relativi alla propria privacy come il maggior problema nell'adozione dei servizi offerti. La raccolta dei dati su larga scala pone ingenti problemi riguardante la privacy e può ostacolare l'adozione da parte di individui che sono molto attenti e scrupolosi alla privacy. La privacy delle informazioni rappresenta una nozione ampia e complessa, in quanto la sua comprensione, ma soprattuto la sua percezione, differisce da individuo a individuo e la sua applicazione richiede sforzi sia legislativi che tecnologici.

Nel 1980, l'OECD (Organisation for Economic Co-operation and Development) ha adottato le linee guida sulla protezione della vita privata e dei flussi transfrontalieri dei dati personali. È considerato una pietra miliare storica in quanto ha rappresentato il primo accordo internazionale sulla protezione della privacy, che rappresentano le basi della maggior parte delle leggi sulla privacy che ha adottato l'Unione Europea successivamente [4].

Solo nel 1995 l'Unione Europea ha approvato la direttiva 95/46/CE in cui gli orientamenti dell'OECD sono stati incorporati per la prima volta in un'influente legge sulla privacy. A differenza degli Stati Uniti, l'Unione Europea si è impegnata a far rispettare le leggi sulla privacy per proteggere in modo completo i dati personali nei suoi paesi membri non solo attraverso i principi, ma anche attraverso la restrizione sul trasferimento dei dati con paesi non appartenenti all'Unione Europea, che a sua volta ne ha influenzato lo sviluppo delle leggi sulla privacy anche in questi paesi.

Successivamente alla direttiva 95/46/CE, nel 2016 l'Unione Europea ha adottato il GDPR (General Data Protection Regulation) che è entrato in vigore nel 2018.

All'interno del GDPR è presente la nozione di Privacy by Design (PbD), vale a dire inglobare le misure sulla privacy e della PET (Privacy Enhancing Technologies) direttamente nella progettazione del software. Tuttavia, il PbD non è mai stato ampiamente utilizzato poiché la maggior parte degli ingegneri trascura l'importanza della privacy o non si assume la propria responsabilità.

Nell'IoT, l'applicazione di ciascun principio all'interno di una legge sulla privacy dovrebbe essere supportata da un insieme di tecnologie (ad esempio PET) in uno o più livelli.

I sistemi Internet of Things esistenti sono progettati utilizzando un'architettura suddivisa a livelli. In un sistema IoT, i dati vengono solitamente raccolti dagli end devices, trasmessi attraverso reti di comunicazione, elaborati dai server locali o remoti ed infine forniti alle varie applicazioni.

Pertanto, i dati personali che attraversano i diversi strati dello stack nell'architettura, necessitano della protezione della privacy su tutti i livelli. È molto importante poter implementare adeguate strategie di protezione della privacy che si basano sui ruoli ricoperti da ciascun livello nel ciclo di vita dei dati.

Le tecniche che sono implementate ad ogni specifico livello, potrebbero divenire insufficienti (qualora in cui la privacy viene violata in altri livelli) oppure potrebbero essere ridondanti (nel caso in cui la privacy è stata protetta da tecniche che sono poi implementate anche in altri livelli). Generalmente, il numero di livelli proposti per l'architettura dell'IoT varia considerevolmente.

In letteratura esistono diverse tipologie di architetture; quella presa in considerazione presenta quattro livelli, che consistono in livello di Sensing, livello di Networking, livello Middleware e livello Application.

L'importanza di ciascun livello nell'architettura a quattro livelli consente di ottenere una visione completa sui diversi livelli di privacy all'interno dell'IoT.

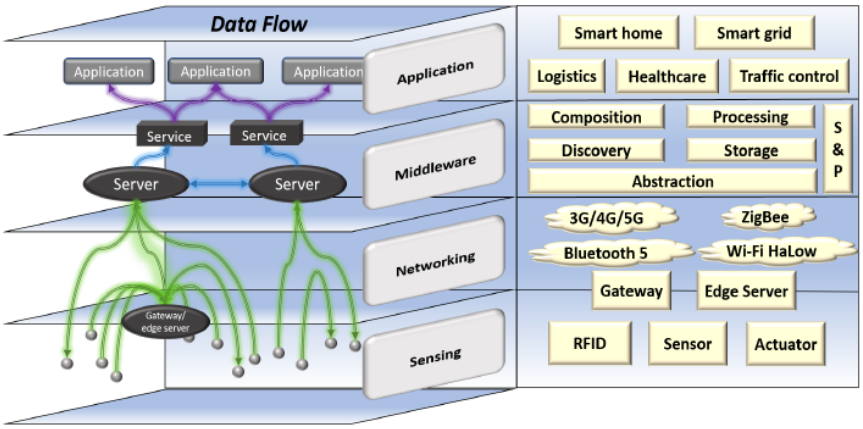

Figura 1 - Architettura IoT di riferimento a quattro strati.

Nella Figura 1 viene mostrata l'architettura di riferimento a quattro livelli. Il livello più basso dell'architettura è rappresentato dal livello di Sensing che permette di colmare il gap tra il mondo fisico e il mondo digitale rendendo identificabili le diverse entità fisiche mediante la tecnologia RFID, rendendole percepibili mediante l'impiego di sensori e controllabili mediante l'ausilio di attuatori.

Il livello di Networking svolge un ruolo fondamentale che consente di collegare lo strato di Sensing con lo strato Middleware, in modo tale che i dati rilevati e i comandi corrispondenti possano essere trasmessi tra i due livelli senza interruzioni. Le principali tecniche che supportano lo strato di networking IoT includono ZigBee, Bluetooth 5, Wi-Fi HaLow e 5G.

Il livello Middleware funziona come se fosse il "cervello" dell'IoT e consente di elaborare i numerosi dati ricevuti dagli strati inferiori. Per far fronte all'interoperabilità tra diversi dispositivi fisici eterogenei, il componente di Abstraction del dispositivo consente di descrivere semanticamente le risorse con un linguaggio coerente come ad esempio XML (eXtensible Markup Language), Resource Description Framework (RDF) o Web Ontology Language (OWL). Procedendo in questo modo, avremo che le risorse potranno essere individualizzate mediante il componente di Discovery delle risorse, che utilizzerà annotazioni semantiche per WSDL e XML Schema (SAWSDL) o semplicemente delle parole chiave. Qualora fosse necessario, per migliorarne la funzionalità, è possibile creare anche più risorse tramite il componente di Composition.

Successivamente, attraverso il componente di Storage, i dati ricevuti possono essere archiviati sul cloud o su database, che sono sempre disponibili all'uso e pronti per essere interrogati. Il componente di Processing è composto invece da diverse unità d'elaborazione e unità analitiche che possono essere combinate tra di loro.

Infine c'è il componente S&P (Security &Privacy), che si occupa della sicurezza e della privacy dei dati, ovvero tutto ciò che riguarda la loro riservatezza, integrità, disponibilità e non ripudio.

Se i dati possono identificare oppure possono rendere identificabile il proprietario, sono necessarie le tecnologie PET per il miglioramento della privacy, affinché si possa proteggere la privacy in accordo ai principi sulla privacy che sono richiesti dalle leggi.

Infine troviamo il livello più alto dell'architettura, che consiste nel livello Application, che contiene le varie applicazioni IoT. A questo livello, a seconda degli scenari in cui vengono raccolti i dati personali, le diverse applicazioni potrebbero incontrare diversi problemi relativi alla privacy.

Dal punto di vista dell'architettura IoT, i dati vengono raccolti dai dispositivi a livello di sensing e trasmessi al livello middleware attraverso il livello di networking, il che discosta i dati dal controllo dei proprietari dei dati.

Per poter assistere correttamente all'interpretazione dei dati, è possibile applicare la nozione di sfera personale, in cui si ha la presenza di un insieme di dispositivi personali e di un gateway, che vengono considerati entrambi affidabili da parte dei legittimi interessati.

La sfera personale è molto importante per poter implementare le quattro strategie di progettazione della privacy data-oriented, in quanto offre una piattaforma affidabile che consente di poter minimizzare, nascondere, separare e aggregare i dati grezzi.

- Minimize: la quantità di dati personali elaborati deve essere limitata al minimo possibile.
- Hide: tutti i dati personali e le loro interrelazioni devono essere opportunamente nascosti.
- Separate: i dati personali devono essere elaborati in modo distribuito e, quando possibile, devono essere elaborati in compartimenti separati.
- Aggregate: I dati personali devono essere elaborati ad un livello di aggregazione più alto e con il minimo dettaglio possibile.

Nella Figura 2.a viene mostrato come può essere creata la sfera personale nel momento in cui vengono raccolti i dati in maniera attiva. Ad esempio, una sfera personale interna è formata dagli elettrodomestici smart e dai router domestici, mentre i dispositivi wearable e gli smartphone compongono una sfera personale esterna.

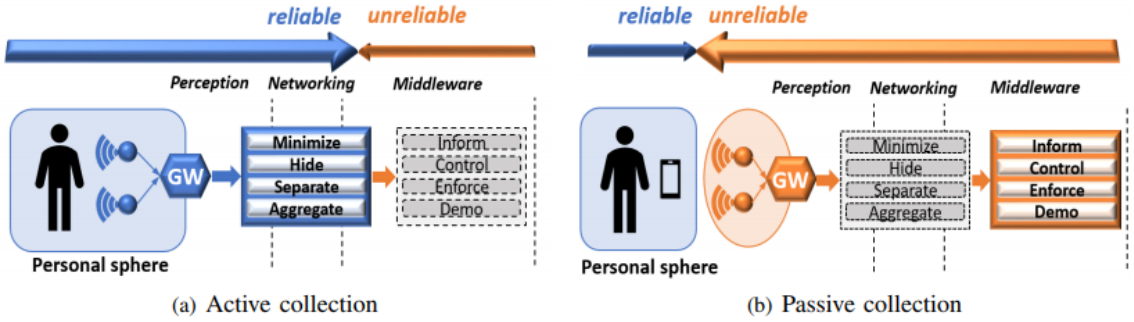

Figura 2 - Framework di protezione della privacy IoT.

Il gateway locale di fiducia (GW) consente agli interessati di poter avviare PET adeguate per elaborare i dati mediante le quattro strategie data-oriented, ma rappresenta un elemento critico all'interno del sistema.

Come mostrato nella Figura 2.b, a causa dell'invisibilità di numerosi dispositivi IoT a livello di sensing, i dati personali potrebbero essere rilevati da dispositivi inaffidabili che sono esterni alla propria sfera personale e i diretti interessati potrebbero essere completamente all'oscuro di questa raccolta passiva dei propri dati perdendone totalmente il controllo già fin dal primo momento [5].

L'INTERNET OF THINGS: CARATTERISTICHE ED EVOLUZIONE NORMATIVA

o LA DISCIPLINA REGOLAMENTARE DELL'INTERNET OF THINGS

Un mondo in continua evoluzione come quello dell'Internet of Things si accosta poco con le esigenze e le tempistiche comportate dall'introduzione di nuove norme. Infatti, non è un caso se la disciplina regolamentare in questo ambito applicativo sia insufficiente o, perlopiù a livello europeo, sia alquanto frammentata nei diversi stati membri, dove le differenti tematiche sono affrontate e gestite in modalità differenti.

Tuttavia, la mancanza di un quadro normativo accurato che sia valido tra tutti gli stati membri, comporta diverse difficoltà, come ad esempio, la discontinuità che potrebbero esserci nello scambio transfrontaliero dei dati, l'eterogeneità che si potrebbe avere nella raccolta e nell'archiviazione dei dati ed ultimo, ma non ultimo per ordine di importanza, il rischio che si possa diffondere in assenza di determinate regole una mancanza di fiducia generale tra i maggiori leader del mercato.

Un panorama frammentato come quello dell'Internet of Things necessita di un quadro regolamentare che sia in grado di armonizzarne la disciplina e, contemporaneamente, riesca a gestire omogeneamente gli eventuali rischi che potrebbero inficiare l'efficienza del funzionamento dei dispositivi IoT, ai danni dell'utente finale. A causa di queste difficoltà, il Regolatore europeo ha cercato di trovare un rimedio per gettare le basi affinché possa esserci un'armonizzazione legislativa dei temi più sensibili e che potessero adattarsi alle evoluzioni sorte con il diffondersi e il progredire dell'Internet of Things.

Nel 2006 la Commissione Europea ha avviato una consultazione pubblica adibita a comprendere le esigenze normative e il quadro regolamentare più idoneo relativo alla produzione e all'utilizzo di "smart chips" basati su tecnologia RFID, affinché potessero sostituire i tradizionali codici a barre, ampliare le possibilità di localizzazione, avviare l'identificazione e la tracciabilità dei dati, ma allo stesso tempo, avrebbero ampliato teoricamente i rischi di violazione della privacy e ridotto la sicurezza dei dati stessi.

Pertanto, l'interesse del Regolatore europeo, era volto ad assicurare la piena diffusione di tale innovazione tecnologica, senza rappresentare alcun danno per gli utenti finali, e aprire così la strada ad un progresso tecnologico sempre più minuzioso, caratterizzato da oggetti interconnessi in un'IoT che avrebbe permesso di "migliorare notevolmente il benessere economico e la qualità della vita". Tutto ciò sarebbe stato possibile soltanto definendo la normativa in materia, nel pieno rispetto della riservatezza dei dati e dei principi etici nella tecnologia. Gli esiti della consultazione furono pubblicati nel 2007, e misero alla luce lo scetticismo da parte del mercato in relazione alla diffusione di una tecnologia del genere senza che vi fossero certezze in merito ai controlli.

Nel corso del triennio 2006-2009 il progresso tecnologico ha conosciuto un ulteriore sviluppo: infatti sono aumentate in maniera significativa le applicazioni che interconnettono gli oggetti sia tra di loro sia ad Internet, variando per numero e tipologia: ad esempio auto collegate ai semafori, elettrodomestici collegati a reti elettriche intelligenti, misuratori di energia elettrica per monitorare e ridurre i consumi.

Per far fronte a questo incremento di dispositivi e per poter regolare in maniera uniforme tale fenomeno, la Commissione Europea nel 2009 ha individuato quattordici azioni che hanno lo scopo di "promuovere lo sviluppo dell'Internet of Things". In tale contesto, la Commissione Europea nel proprio action plan individua quattordici ambiti di intervento:

- costruzione di un assetto di governance per la gestione dell'Internet of Things;
- gestione degli impatti rispetto alla disciplina della privacy e della sicurezza dei dati;

- necessità di garantire agli utenti il “diritto al silenzio dei dispositivi”, permettendo loro di eliminare i dati condivisi e disconnettersi in qualsiasi momento dagli oggetti collegati ad Internet;
- predisposizione di azioni idonee a garantire la sicurezza e la privacy dei dati;
- sviluppo di Internet of Things come risorsa essenziale per la crescita dell’Europa;
- definizione di linee guida standard al fine di uniformare la disciplina dell’Internet of Things;
- finanziamento della ricerca;
- sviluppo delle “Public Private Partnership” al fine di incrementare l’Internet of Things;
- diffusione di progetti pilota per assicurare il grado di innovazione più alto possibile;
- avvio di tavoli di lavoro con le istituzioni europee (Parlamento Europeo e Consiglio);
- condivisione di informazioni e piani strategici di sviluppo con i partner internazionali;
- impatto ambientale per il riciclo delle tecnologie RFID;
- analisi di mercato relative agli utilizzi delle tecnologie RFID;
- monitoraggio dell’evoluzione normativa dell’Internet of Things.

La Commissione Europea, alla luce delle potenziali criticità presentate dall’IoT e dalla vasta portata degli interventi che avrebbe richiesto lo sviluppo delle 14 linee d’azione, ha proseguito nella definizione del background regolamentare che fosse il più possibile aderente ai principi dell’Unione Europea e, nel 2012, ha avviato un’ulteriore consultazione sulle regole per gli smart device connessi. Tale intervento mirava ad 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 come i modelli inerenti al comportamento degli utenti, le proprie preferenze ed infine l’ubicazione.

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. Nel settembre del 2016 fu così costituita AIOTI grazie al supporto di alcune industrie del settore.

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 di condividere spunti di riflessione e sul come procedere in tale ambito. Questa iniziativa è stata avviata ed implementata contestualmente con la creazione di un mercato unico europeo del digitale: il “Digital Single Market” (DSM).

La necessità di costruire un mercato unico dell’IoT può essere definito come 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 tutti insieme nonostante i volumi di dati scambiati. Affinché possa essere gestita una tale mole di dati, nel 2017 è stata avviata l’iniziativa europea “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.

Nell’aprile 2018 la Commissione Europea ha riconosciuto l’esigenza di creare un framework normativo stabile e armonizzato a livello europeo. In particolare, ha sollecitato la definizione di regole chiare in materia di responsabilità in caso di evento dannoso a carico degli utenti di connected devices, 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, con lo scopo di avere un modo più efficiente su come approcciarsi al mercato [6][7].

o INTERNET OF THINGS E GDPR

Il regolamento generale sulla protezione dei dati (General Data Protection Regulation, GDPR), approvato ufficialmente come regolamento UE n. 2016/679, è il più recente regolamento in vigore in materia di trattamento dei dati personali, entrato in vigore il 25 maggio 2016 ed operativo dal 25 maggio 2018 [7].

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 approvato le norme incompatibili della protezione dei dati personali precedentemente in vigore (D. Lgs. N. 196/2003) [8].

L'art. 5 del GDPR stabilisce dei principi fondamentali riguardanti il trattamento dei dati personali che fanno da base all'intera normativa. Tali principi sono:

- **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 che non siano 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 accidentale.
- **Principio di responsabilizzazione (accountability)**: Il titolare del trattamento è competente per il rispetto dei principi precedenti ed è in grado di comprovarlo. Questo principio stabilisce che il titolare è tenuto ad adottare dei comportamenti proattivi in grado di assicurare il rispetto del regolamento [9].

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.

- *Privacy by default* (privacy come impostazione predefinita): Stabilisce che le imprese dovrebbero gestire i dati personali considerando solamente il trattamento dei 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).

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.

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 [10] [11].

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, di responsabile, di Data Protection Officer (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 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 dispositivi 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 potrebbero derivare.

È necessario effettuare anche la valutazione sull'impatto del trattamento, se si ritiene che possa presentare rischi elevati, o nei casi descritti precedentemente in cui risulti obbligatoria.

Essendo fortemente correlata all'uso di IoT o dei Big Data (o in sistemi che integrano entrambe le tecnologie, dovendo fare uso di enormi moli di dati), 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 [12].

o ORGANIZZAZIONE E RUOLI

Sebbene il nuovo regolamento possa essere specifico per l'Unione Europea, la sua portata ed il suo impatto sono globali. Le imprese di tutti i paesi che raccolgono, archiviano o elaborano i dati personali dei cittadini dell'Unione Europea, siano essi clienti, dipendenti, pazienti, assicurati, beneficiari, appaltatori, terze parti, volontari o visitatori, dovranno dimostrare la conformità al GDPR.

Il GDPR descrive chiaramente i ruoli e le responsabilità delle entità coinvolte nella raccolta, nell'archiviazione e nel trattamento dei dati personali. Suddivide queste entità in:

- Data Controller (il titolare del trattamento dei dati);
- Data Processor (il responsabile del trattamento dei dati);
- Data Protection Officer o DPO (il responsabile della protezione dei dati personali);

La tecnologia può aiutare i data controller, i data processor e i DPO a soddisfare con successo i loro requisiti di conformità.

L'articolo 4 del GDPR definisce il titolare del trattamento (*data controller*) come "una persona fisica o giuridica, pubblica amministrazione, agenzia, associazione o qualsiasi altro ente, che da solo o in collaborazione con altri, determina le finalità, le modalità e gli strumenti utilizzati nell'ambito del trattamento di dati personali, comprese le decisioni riguardanti la sicurezza".

Il titolare del trattamento potrebbe essere un'organizzazione (ad esempio una banca, un rivenditore) oppure potrebbe essere un individuo (ad esempio un medico di famiglia) che raccoglie ed elabora le informazioni sui clienti, sui pazienti, ecc.

In base al GDPR, il responsabile del trattamento dei dati è una figura distinta da chi gestisce i dati; è una figura 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, cioè è responsabile di garantire che i dati siano trattati nel rispetto dei principi di liceità, correttezza, trasparenza, minimizzazione dei dati, accuratezza, limitazione dello spazio di archiviazione, integrità e riservatezza. 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, viene definito sempre nell'articolo 4 del GDPR, come "una persona fisica o giuridica, pubblica amministrazione, agenzia associazione o altro ente che elabora i dati personali per conto di un titolare del trattamento".

I responsabili del trattamento dei dati potrebbero includere organizzazioni quali fornitori di servizi cloud e data analytics provider. 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.

Nonostante i titolari del trattamento si relazionano ai responsabili del trattamento, essi sono anche direttamente responsabili della protezione dei dati nell'ambito del GDPR. Tra l'altro, i responsabili del trattamento possono anche essere titolari del trattamento. Ad esempio, un venditore che conduce ricerche di mercato per un'altra azienda sarebbe un responsabile al trattamento dei dati, ma quando si gestiscono i dati dei propri dipendenti assumono il ruolo di titolare del trattamento dei dati.

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) [13][14].

o ACCOUNTABILITY

Nella versione in lingua inglese del GDPR (articolo 5 comma 2) si rinviene il principio di "accountability" come criterio guida del regolamento per la protezione dei dati personali. In italiano può essere tradotto con il termine "responsabilizzazione", ma non è possibile interpretare il concetto solo come "responsabilità", perché sarebbe molto limitativo e non conforme pienamente all'approccio voluto invece dal legislatore. Il termine "accountability" è di uso comune nel mondo anglosassone e viene utilizzato nel mondo della finanza, della revisione dei conti e in altri settori specifici. Definire praticamente cosa significhi esattamente "accountability" è molto complesso. Lo si potrebbe tradurre con "rendicontabilità".

Nell'ambito della tutela e protezione dei dati personali il concetto di accountability assume un ruolo fondamentale, perché rappresenta la chiave di lettura e di interpretazione sul giusto comportamento che il titolare del trattamento deve adottare davanti ad un quesito, ad un problema, oppure riguardo i dubbi sul corretto processo organizzativo o tecnico alla base di un trattamento dei dati.

In letteratura inglese i due termini responsabilità e accountability non sono esattamente equivalenti. Il concetto di "responsibility" è legato al dover agire, mentre il concetto di "accountability" è legato al rendere conto dell'azione fatta, al rendere conto dei risultati ottenuti (sia delle cose fatte bene che eventualmente di quelle fatte male).

La complessità intrinseca dell'IoT non si adatta facilmente ai tradizionali costrutti legali e normativi. Gli effetti della legge sono mediati sia dall'interazione con altre leggi sia dalle persone che sono coinvolte. Questo significa che è difficile attribuire la responsabilità fino a quando non vengono scoperti i rischi di qualsiasi nuova tecnologia a seguito dell'utilizzo.

L'aspetto legale più importante per quanto concerne l'accountability è rappresentato dalla trasparenza del funzionamento di un sistema. Ad esempio, se un produttore tecnologico ha causato dei danni oppure delle

perdite a un utente, è obbligato a dimostrare che ha agito in maniera ragionevole, altrimenti sarà ritenuto responsabile. Se la tecnologia non funziona correttamente, indipendentemente a chi verrà attribuita la colpa, la maggior parte delle questioni di responsabilità nel mondo IoT, probabilmente deriveranno dall'acquisizione e dall'elaborazione delle informazioni.

La legge regola le azioni delle persone giuridiche, compresi individui e società, ma non le tecnologie stesse. Pertanto, un punto chiave dell'accountability dell'IoT è rappresentato dalla decisione di utilizzare una specifica tecnologia IoT oppure il modo in cui assemblare o integrare i vari componenti;

La trasparenza dipende dall'entità, ad esempio, gli utenti IoT ignorano il funzionamento di una tecnologia, rendendola di fatto una black box, le uniche opzioni effettuate dagli utenti saranno quelle di fidarsi della tecnologia oppure, in altri casi, di non utilizzarla poiché generalmente non possono sapere in anticipo quali potrebbero essere i potenziali guasti; contrariamente invece, a quanto accade con un produttore, in cui le leggi generalmente considerano che debba conoscere in anticipo ciò che potrebbe essere scoperto a posteriori in caso di fallimento, questo perché si presuppone che vengano effettuati processi di test e di valutazione. Gli utenti che compongono i propri sistemi mediante l'aggregazione di più componenti standard, possono essere considerati in un certo senso dei produttori. Il livello di trasparenza richiesto per questa categoria di utenti è fondamentalmente diverso da quello che dovrebbe essere richiesto invece ai produttori standard. I requisiti legali affinchè possa essere inglobata la trasparenza nelle tecnologie IoT devono tenere conto delle differenti prospettive. La tecnologia può aiutare ad abilitare l'accountability nell'IoT, in particolare perché l'IoT e i suoi ecosistemi sono ancora in via di sviluppo.

Anche se la tecnologia non sarà una panacea, può integrare e rafforzare altri meccanismi di accountability come ad esempio leggi, quadri di governance istituzionali e standard [15].

o NORMATIVE E I PUNTI DI ATTENZIONE

Affinché possa esserci uno sviluppo sostenibile dell'IoT, gli organi decisionali politici ed economici devono sviluppare regolamenti adeguati ad essere in grado di controllare l'uso equo dell'IoT nella società. Per l'ambito dell'IoT dovrebbero includere:

- normative per i connected devices.
- normative riguardanti le reti e la loro rispettiva sicurezza.
- normative per i dati associati ai dispositivi.

Le principali leggi e normative riguardanti l'IoT che attualmente sono esistenti nell'Unione Europea e negli USA rappresentano anche le linee guida per la maggior parte dei paesi sviluppati e in via di sviluppo, che presentano leggi simili o equivalenti.

L'Unione Europea ha iniziato l'attività nell'area IoT nel 2005 quando fu lanciato "2010: A European Information Society for Growth and Employment" che definisce le politiche per lo sviluppo dell'European Information Space e comporta innovazione e investimenti in ricerca e sviluppo per ottenere migliori azioni e servizi sulla qualità della vita.

Successivamente, l'Unione Europea ha promulgato le seguenti normative e iniziative che riguardano principalmente i dati, le reti, la sicurezza e i devices:

- EU DPR-2012: Regolamento europeo sulla protezione dei dati.

Lo scopo di questo regolamento è quello di garantire la protezione dei "dati personali" delle persone indipendentemente dal tipo di trattamento in corso. I dati personali includono tutti i dati che possono essere riferiti ai singoli, il che implica che il concetto di dati individuali può estendersi a vaste aree dell'IoT.

- Direttiva EU 2013/40: la presente direttiva riguarda i "cyber crimini", cioè gli attacchi lanciati contro i sistemi di informazione. Fornisce definizioni di reati e stabilisce sanzioni adeguate a chi commette degli attacchi contro i sistemi di informazione.

- Direttiva EU NIS-2016: questa direttiva sulla sicurezza delle reti e dell'informazione (NSI - Network and Information Security) riguarda argomenti di "Cybersecurity". Il suo scopo è quello di fornire misure legali per assicurare un livello generale di sicurezza informatica comune nell'Unione Europea e un grado di coordinamento rafforzato tra i membri dell'Unione Europea.

- Direttiva EU 2014/53: la direttiva “On the harmonization of the laws of the member states relating to the marketing of radio equipment” riguarda la questione della standardizzazione, che è molto importante per lo sviluppo congiunto e armonizzato della tecnologia all’interno dei paesi membri dell'Unione Europea.

- EU GDPR: European General Data Protection Regulation-2016. Il presente regolamento riguarda la privacy, la proprietà e la protezione dei dati e sostituisce l'EU DPR-2012. Fornisce un insieme di regole direttamente applicabili negli stati membri dell'Unione Europea.

- Iniziativa EU Connected Communities: questa iniziativa riguarda lo sviluppo dell'infrastruttura dell'IoT e mira a raccogliere informazioni dal mercato riguardo i progetti di connettività pubblica e privata esistenti che cercano di fornire banda larga ad alta velocità (oltre 30 Mbps).

- Iniziativa Europe 2020 "Innovation Europe": questa iniziativa fornisce la struttura del programma per finanziare nuovi progetti (sia IoT che altri) come "Horizon 2020". Una delle sette parti della strategia Europe 2020 per una crescita intelligente, sostenibile e inclusiva è la "Innovation Union" (IU), che persegue diverse azioni per ottenere tre obiettivi:

    1. Trasformare l'Europa in uno dei migliori attori in ambito scientifico a livello mondiale.
    2. Rendere l'innovazione libera da ostacoli quali i brevetti costosi, la frammentazione del mercato e la carenza di competenze.
    3. Rivoluzionare il modo in cui cooperano i settori pubblico e privato e potenziare le partnership tra istituzioni europee, autorità (nazionali e regionali) ed imprese.

Per quanto riguarda invece gli Stati Uniti, la legislazione generale dedicata all'IoT include quanto segue:

- White House Initiative 2012: lo scopo di questa iniziativa è quello di specificare un quadro per proteggere la privacy del consumatore in una rete in ambito lavorativo. Questa iniziativa comporta una relazione sulla "Carta dei diritti dei consumatori", che si basa sui cosiddetti "principi di correttezza delle informazioni" (FIPP).

- IoT Cybersecurity Improvement Act 2017: si tratta di una proposta di legge davanti al Senato degli Stati Uniti che mira a migliorare la sicurezza dei dispositivi connessi ad Internet. Il disegno di legge definisce i dispositivi IoT come un qualsiasi dispositivo che è connesso ed utilizza Internet.
  Il disegno di legge non pone dei requisiti sui produttori di tali dispositivi, ma segue un altro approccio, cioè, indirizza le agenzie governative a includere alcune clausole nei loro contratti che richiedono funzionalità di sicurezza per tutti i dispositivi connessi ad Internet e che saranno acquisiti dal governo degli Stati Uniti. La proposta di legge descrive quali sono queste clausole e in che modo è possibile ottenere una deroga a queste funzionalità richieste e richiede che i dispositivi da vendere si basino su standard internazionali (come ad esempio ISO, NIST, ecc.) [16].

o DATA PROTECTION

Il 2018 è stato un anno determinante per la Data Protection poiché è entrato in vigore integralmente il GDPR. È emersa con chiarezza, per la prima volta, la relazione che esiste tra protezione dei dati personali con le libertà e i diritti degli interessati.

Il primo caso di incidente relativo alla Data Protection è rappresentato dal caso di Cambridge Analytica, collegato da un lato con le elezioni presidenziali americane e dall'altro lato al calo del valore in borsa di Facebook.

L'opinione pubblica non tollera benevolmente un trattamento illecito di dati personali e tuttociò può avere conseguenze rilevanti per la democrazia degli Stati Uniti.

Nei primi mesi del 2019 l'Unione Europea ha mostrato discrete preoccupazioni riguardo le possibili interferenze esterne con le prossime elezioni europee. L'Unione Europea ha consolidato con il GDPR una leadership mondiale incontestabile e nel 2018 anche la California ha adottato una legge statale sulla protezione dei dati personali che è molto simile al GDPR.

Attualmente i dati personali rappresentano la materia prima del business. Conoscere e saper interpretare in anticipo le preferenze, le aspettative, le abitudini, i comportamenti, le propensioni delle persone, fa la differenza e rappresenta il target che guida le scelte di mercato.

La Data Protection 4.0 rappresenta il periodo in cui le nuove regole consentono di sviluppare in modo conforme al GDPR e alla sensibilità del pubblico. Per la fase data protection 4.0, diventano cruciali altri articoli del GDPR:

- L'art. 25 (Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita), l'art. 35 (Valutazione d'impatto sulla protezione dei dati) e l'art. 36 (Consultazione preventiva) che governano complessivamente il processo di innovazione;
- L'art. 32 (Sicurezza del trattamento), l'art. 33 (Notifica di una violazione dei dati personali all'autorità di controllo) e l'art. 34 (Comunicazione di una violazione dei dati personali all'interessato) che disegnano il presidio e la gestione della sicurezza dei dati personali;
- L'art. 28 (Responsabile del trattamento) che ridisegna il rapporto fra il titolare e la sua catena di fornitura, l'ecosistema produttivo e di servizi che gli consente di svolgere il suo ruolo [17].

I connected devices vengono utilizzati sempre più spesso anche per lo scambio di dati personali e riservati, introducendo ulteriori questioni per quanto riguarda l'adeguamento alla normativa europea in materia di protezione dati. Internet of Things e data protection camminano sempre più di pari passo. È evidente l'importanza di proteggere i sistemi IoT utilizzando protocolli di comunicazione sicuri e metodi di cifratura sufficientemente robusti. Due aspetti di sicurezza che vengono spesso sottovalutati creando di fatto delle vulnerabilità che aprono dei varchi pericolosi nelle aziende.

L'Open Web Application Security Project (OWASP) ha recentemente rilasciato la "OWASP IoT-Top Ten 2018", nell'ambito del progetto OWASP Internet of Things, in cui vengono elencate le 10 cose da evitare durante la creazione, la distribuzione e la gestione dei sistemi IoT:

1. Password deboli, facilmente indovinabili o preimpostate;
2. Servizi di network non sicuri;
3. Interfacce di sistema non sicure;
4. Aggiornamenti non sicuri e non affidabili;
5. Utilizzo di componenti non sicuri o obsoleti;
6. Privacy e data protection insufficienti;

7. Trasferimenti e conservazione di dati non sicuri;
8. Cattiva gestione dei dispositivi e dei servizi ad essi collegati;
9. Impostazioni di default non sicure;
10. Mancanza di misure di “Physical Hardening”.

Lo scopo di questo elenco, è quello di aiutare produttori, sviluppatori e consumatori a comprendere meglio i problemi di sicurezza associati all’Internet of Things, fornendo al contempo agli utenti, in qualsiasi contesto si trovino, gli strumenti giusti per prendere le migliori decisioni di sicurezza durante la creazione, l’implementazione o la valutazione delle tecnologie IoT [18].

o IoT Security Assessment

Il programma di certificazione "IoT Security Assessment" introdotto dalla GSMA (Groupe Spéciale Mobile Association)[1] mira a valutare e certificare i dispositivi IoT in base a criteri specifici di sicurezza.

Questo programma è stato istituito per affrontare le preoccupazioni crescenti riguardo alla sicurezza dei dispositivi IoT, riconoscendo la necessità di standardizzazione e di requisiti minimi di sicurezza per proteggere i dispositivi connessi e i dati che essi gestiscono.

Le principali caratteristiche e obiettivi del programma di certificazione "IoT Security Assessment" includono:

1. **Valutazione della sicurezza:** Il programma prevede una valutazione dettagliata della sicurezza dei dispositivi IoT, esaminando vari aspetti quali la crittografia dei dati, i meccanismi di autenticazione, le procedure di aggiornamento del firmware, la gestione delle chiavi di sicurezza e la protezione dalla manipolazione e dagli attacchi informatici.
2. **Standardizzazione e requisiti minimi:** Il programma definisce standard e requisiti minimi di sicurezza che i dispositivi IoT devono soddisfare per ottenere la certificazione. Ciò aiuta a garantire un livello di sicurezza adeguato a prevenire vulnerabilità e minacce alla sicurezza dei dati.
3. **Certificazione e marchio di conformità:** I dispositivi che superano con successo la valutazione della sicurezza ricevono una certificazione e possono esibire il marchio di conformità "IoT Security Assessment" della GSMA. Questo marchio fornisce un'indicazione ai consumatori e agli operatori di rete che il dispositivo ha superato determinati standard di sicurezza.
4. **Promozione della sicurezza nell'ecosistema IoT:** Il programma mira anche a promuovere la sicurezza nell'ecosistema IoT, incoraggiando i produttori a adottare buone pratiche di sicurezza fin dalla fase di progettazione e sviluppo dei dispositivi.

È importante notare che il programma "IoT Security Assessment" della GSMA è progettato per essere un'iniziativa collaborativa che coinvolge produttori, fornitori di servizi, regolatori e altre parti interessate nell'industria dell'IoT. L'obiettivo è creare un ambiente in cui i dispositivi IoT possano essere sviluppati, prodotti e distribuiti conformemente a standard di sicurezza ben definiti.

Poiché le informazioni e i dettagli specifici sul programma possono essere soggetti a modifiche nel tempo, è consigliabile consultare direttamente le risorse ufficiali della GSMA o del programma "IoT Security Assessment" per le informazioni più aggiornate e dettagliate sui criteri di certificazione e sui requisiti di sicurezza.

[1] https://www.gsma.com/iot/iot-security-assessment/

o Health Insurance Portability and Accountability Act

A seconda dell'ambito in cui vengono impiegati i dispositivi IoT, possono essere rilevanti leggi e regolamenti specifici. Ad esempio, nell'ambito della sanità (Healthcare), possono essere applicabili normative come la Health Insurance Portability and Accountability Act (HIPAA)[2] negli Stati Uniti, che stabilisce requisiti specifici per la sicurezza dei dati sanitari. La Health Insurance Portability and Accountability Act (HIPAA) è una legge federale degli Stati Uniti promulgata nel 1996 con l'obiettivo di migliorare l'accesso alla copertura sanitaria, la portabilità dei piani sanitari e di stabilire normative per la sicurezza e la privacy dei dati sanitari dei pazienti.

La HIPAA è stata creata con diverse finalità principali:

- Portabilità dell'assicurazione sanitaria: Garantisce ai lavoratori e ai loro familiari la continuità della copertura sanitaria quando cambiano lavoro o perdono il lavoro.
- Riduzione dell'abuso e della frode nell'assistenza sanitaria: Introduce disposizioni per ridurre la frode e l'abuso nei programmi di assistenza sanitaria, stabilendo regole e procedure per la condivisione e l'utilizzo dei dati sanitari.
- Sicurezza e privacy dei dati sanitari: La HIPAA include la "Privacy Rule" e la "Security Rule" per garantire la sicurezza e la riservatezza dei dati sanitari dei pazienti. La "Privacy Rule" stabilisce standard nazionali per la protezione dei dati sanitari identificabili, limitando la divulgazione e l'uso di tali informazioni. La "Security Rule" richiede ai fornitori di servizi sanitari e agli operatori sanitari di implementare misure di sicurezza tecniche, amministrative e fisiche per proteggere i dati sanitari elettronici.

La HIPAA si applica a diverse entità coinvolte nella gestione e nell'elaborazione delle informazioni sanitarie, inclusi i fornitori di assistenza sanitaria (ospedali, medici, cliniche), le compagnie assicurative sanitarie, i fornitori di servizi sanitari, i gestori dei dati sanitari e tutti coloro che hanno accesso ai dati sanitari protetti.

Le violazioni della HIPAA possono comportare sanzioni pesanti e multe significative per le organizzazioni che non rispettano le disposizioni di sicurezza e privacy dei dati sanitari. Inoltre, la legge prevede procedure di notifica delle violazioni che richiedono alle organizzazioni coinvolte di notificare tempestivamente ai pazienti e alle autorità competenti le violazioni dei dati sanitari. È fondamentale che le organizzazioni coinvolte nella gestione dei dati sanitari comprendano appieno e rispettino le disposizioni della HIPAA per garantire la sicurezza e la riservatezza dei dati dei pazienti. L'implementazione di misure di sicurezza e la formazione del personale sono fondamentali per conformarsi alle regole e alle disposizioni della legge HIPAA.

LA PROPRIETA' INTELLETTUALE

Affinché possano esserci efficaci strategie gestionali, commerciali e di innovazione è necessario introdurre dei meccanismi di protezione degli oggetti che sono frutto dell'inventiva e dell'ingegno umano. La proprietà intellettuale indica proprio i principi giuridici che mirano a tutelare i frutti dell'inventiva e dell'ingegno umano.

Gli strumenti che consentono di garantire la proprietà intellettuale sono i brevetti, i marchi ed il copyright. In particolare il brevetto è un titolo giuridico di proprietà a tutela del titolare dell'invenzione che concede il diritto esclusivo di realizzare l'invenzione e di sfruttarla secondo le condizioni stabilite dalla legge. Il marchio invece indica un qualunque segno suscettibile di rappresentazione grafica o percepibile attraverso i sensi, che permette di distinguere prodotti o servizi di un'impresa da quelli delle altre. Infine Il copyright è un meccanismo di protezione applicabile alle opere soggette a diritto d'autore.

[2] https://www.cdc.gov/phlp/publications/topic/hipaa.html

Le tre tecnologie emergenti che guideranno gli investimenti in ambito IT nei prossimi anni sono Internet of Things, Blockchain e l'intelligenza artificiale. Dal punto di vista della tutela della proprietà intellettuale, i produttori di queste tecnologie si troveranno ad affrontare sfide di notevole complessità. Questi dispositivi rappresentano molto spesso un prodotto collaborativo tra componenti, tecnologie e software che sono realizzati da molte aziende diverse.

Alcuni esperti dell'IBA (International Bar Association) hanno evidenziato come può essere tutelata la proprietà intellettuale di ogni componente, caratteristica e funzionalità di questi dispositivi. Per esempio, possono essere oggetto di brevetto la funzionalità stessa del dispositivo oppure i circuiti integrati e i microchip. Il software che consente al prodotto di funzionare, può essere coperto dal diritto d'autore. Mentre i database a cui si collegano questi dispositivi possono essere doppiamente tutelati: la stessa tecnologia di archiviazione può essere brevettata, così come è possibile estendere il diritto d'autore alla struttura organizzativa del database [19].

La presenza di un'enorme quantità di dati raccolti ed elaborati dai nodi dell'Internet of Things fa sorgere il problema di stabilire a chi appartengano questi dati e come bisogna proteggerne la privacy.

I dispositivi IoT, per come sono stati progettati, devono scambiare i propri dati con quelli di un altro dispositivo. Questo flusso di informazioni rende di per sé impraticabili le soluzioni di tutela della protezione dei dati. Proprio per questo motivo, le aziende dovrebbero prestare maggiore attenzione alle criticità del loro business, elaborando strategie personalizzate in base a quelle che sono le informazioni scambiate.

Si potrebbero brevettare anche le tecnologie di connessione, i protocolli di trasmissione e le soluzioni di sicurezza adottate. Infine, non bisogna dimenticare che tutte le tecnologie possono essere oggetto di reverse engineering e quindi bisognerebbe anche pensare a garantire una protezione adeguata del proprio segreto industriale.

o STRUMENTI DI TUTELA NELL'ERA DELL'INTERNET OF THINGS

Nel dicembre 2016 si è svolto un convegno dal titolo "IoT un'opportunità per l'industria 4.0 ed una sfida per la tutela della proprietà intellettuale" organizzato dal comitato italiano Business Software Alliance (BSA) in collaborazione con Confindustria.

Si tratta di un evento riguardante l'ambito dell'IoT in cui sono state poste sotto analisi le conseguenze per lo sviluppo della competitività per le imprese italiane. Inoltre è stato affrontato il tema su come le tecnologie abilitanti per l'IoT possano rappresentare uno strumento efficace ed innovativo per difendere la proprietà industriale, intellettuale e i dati dei cittadini e dei consumatori [20].

In relazione alle norme di proprietà intellettuale, la Blockchain può essere utilizzata per creare una nuova modalità di registri pubblici di proprietà industriale, oltre a servizi di protezione per segreti industriali.

La Blockchain può influenzare il mondo dei diritti di proprietà intellettuale anche indirettamente, dal momento che è anche la tecnologia alla base per gli smart contracts, o "contratti intelligenti".

A livello europeo opera l'Ufficio Europeo per la Proprietà Intellettuale (EUIPO), che è fortemente intenzionato a esplorare il potenziale delle tecnologie informatiche e in maniera particolare quella Blockchain. Infatti, a giugno 2018, ha lanciato il primo Blockhackton al mondo per contrastare contraffazione e pirateria. La soluzione perfetta ad un simile problema è rappresentata appunto dalla tecnologia Blockchain, che rappresenta uno degli elementi dirompente nell'ambito IoT.

Nel 2009 una persona ignota, conosciuta sotto il nome di Satoshi Nakamoto, diffonde un documento dal titolo "Bitcoin: a peer-to-peer electronic cash system" in cui espone una versione peer-to-peer della moneta elettronica che permette ai pagamenti online di essere spediti direttamente da una parte all'altra senza l'intervento di un'istituzione finanziaria che funga da intermediario, questa tecnologia sottostante si chiama appunto Blockchain, che è alla base del funzionamento del Bitcoin.

Nel corso degli ultimi anni le Blockchain hanno dimostrato di poter svolgere numerose altre funzioni. Può essere utilizzata per gestire qualsiasi scambio, contratto, accordo, per tracciare ed ovviamente per pagare. Ogni volta che un prodotto viene movimentato, la transazione può essere documentata, creando una storia permanente del prodotto stesso, dalla produzione alla vendita. Ciò potrebbe ridurre drasticamente i ritardi di tempo, i costi aggiuntivi e l'errore umano che oggi affliggono i processi di supply chain.

Una Blockchain permette di creare un sistema decentralizzato per le transazioni in cui la fiducia risiede nell'intera piattaforma, questo perché è il sistema stesso, formato dai nodi e dal network di utenti, che garantisce all'utente la sicurezza e l'integrità della transazione. Sostanzialmente è un database strutturato e distribuito che è replicato e condiviso tra i membri di un network.

Questo network è formato da un set di nodi che formano una rete peer-to-peer che operano sulla stessa Blockchain e che fungono da punto d'ingresso per altri utenti. La fiducia e il controllo nelle transazioni basate su Blockchain non sono a scatola chiusa, ma il tutto avviene in maniera trasparente.

Il problema di verificare la legittimità di una transazione in assenza di un'autorità centrale che effettua i dovuti controlli, viene risolto decentralizzando appunto il libro mastro, in modo che ogni utente sia in possesso di una copia. Chiunque può chiedere che una transazione sia aggiunta alla Blockchain, ma tale richiesta sarà accettata solo se tutti gli utenti saranno concordi in merito alla sua legittimità, cioè solo ed esclusivamente nel momento in cui la richiesta provenga dalla persona autorizzata. Questo controllo viene eseguito in modo affidabile e automatico per conto di ciascun utente, creando un sistema di libro mastro molto rapido e sicuro, fortemente in grado di resistere a eventuali manomissioni.

Il termine Blockchain viene attribuito dal principio di funzionamento su cui si basa questa tecnologia; infatti ogni nuova transazione da registrare viene unita ad altre nuove transazioni per formare un "blocco", che viene aggiunto come ultimo anello di una lunga "catena" di transazioni cronologiche che forma il libro mastro Blockchain detenuto da tutti gli utenti.

Questo lavoro è detto "mining" è può essere svolto dai "miner". Qualunque utente può diventare un "miner" e competere per essere il primo a risolvere il complesso problema matematico legato alla creazione di un blocco di transazioni valido e crittografato da aggiungere alla Blockchain. Quando viene aggiunto un nuovo blocco alla catena viene aggiornato il libro mastro che è detenuto da tutti gli utenti. Gli utenti accettano un nuovo blocco solo dopo che è stata verificata la validità di tutte le sue transazioni. Se viene rilevata un'anomalia, il blocco viene rifiutato, altrimenti viene aggiunto e rimarrà nella catena come record pubblico permanente, infatti nessun utente potrà più rimuoverlo.

A questo punto è logico intuire che non può esistere un "falso libro mastro", poiché tutti gli utenti sono in possesso di una versione autentica che possono utilizzare per poter effettuare un confronto.

Le potenzialità di una tecnologia del genere, in cui vengono registrate le informazioni in maniera indelebile ed immodificabile all'interno di un database pubblico e accessibile, non ha applicazioni solo nel campo finanziario. Proprio per questo motivo Blockchain potrebbe diventare una nuova infrastruttura per gli scambi basata su un sistema decentralizzato, analogamente al ruolo avuto dal protocollo TCP/IP in Internet.

Una delle applicazioni più interessanti nel mondo Blockchain è rappresentato dallo smart contracting. Uno smart contract è sostanzialmente un contratto, scritto in un linguaggio che è eseguibile da un computer, che è in grado di entrare in esecuzione automatica e fare rispettare le proprie clausole senza alcun intervento esterno.

Lo *smart contract code* è registrato su una Blockchain e quindi ne sfrutta tutte le particolari potenzialità. Uno *smart legal contract* è l'utilizzo di uno smart contract code per articolare, verificare ed applicare un accordo tra più parti. I tre elementi caratteristici sono l'autonomia, l'autosufficienza e la decentralizzazione. Autonomia significa che un contratto, dopo essere stato eseguito, non richiede un successivo contatto tra le parti contraenti. Uno smart contract è invece autosufficiente nel senso che ha l'abilità di gestire le proprie risorse, cioè in base alle necessità richieste guadagna le risorse necessarie per portare a termine un obiettivo.

Infine gli smart contract sono decentralizzati e non fanno affidamento su un server centralizzato, in modo da essere distribuiti ed eseguiti all'interno dei nodi della rete.

La protezione delle proprietà intellettuali sarebbe un ambito ad alto impatto se tecnologie come la Blockchain o gli Smart Contracts fossero più diffuse.

Questa tecnologia può essere impiegata in diversi contesti IoT:

- **Sicurezza e autenticazione:** Le blockchain consentono l'implementazione di protocolli di autenticazione sicuri per garantire che solo dispositivi autorizzati possano accedere e comunicare sulla rete IoT.
- **Tracciabilità e gestione della catena di approvvigionamento:** Nell'ambito della logistica e della supply chain, le blockchain consentono una tracciabilità completa dei prodotti lungo l'intera catena, riducendo i rischi di frodi o manipolazioni.
- **Pagamenti e micro-transazioni:** Le blockchain possono facilitare i micro-pagamenti automatici tra dispositivi IoT, consentendo una maggiore automazione e l'implementazione di modelli di business basati su economie di condivisione.
- **Privacy e gestione dei dati:** Le blockchain permettono ai proprietari di dispositivi IoT di mantenere il controllo sui propri dati, stabilendo regole e permessi di accesso tramite smart contract che definiscono chi può accedere a determinati dati e per quanto tempo.

Tuttavia, è importante notare che l'implementazione delle Blockchain nell'IoT presenta anche sfide come la scalabilità, i costi e la complessità operativa. L'adattamento e lo sviluppo di standard e protocolli comuni sono essenziali per garantire l'interoperabilità tra i dispositivi e le reti Blockchain.

Nel campo dei Big Data generati nell'ambito IoT, la Blockchain potrebbe essere utilizzata per definire la paternità dei dati e la conseguente protezione e valorizzazione per un modello economico. I dati potrebbero diventare degli asset digitali che, se protetti, potrebbero generare un ritorno economico per gli utenti. La valutazione economica sarebbe possibile grazie alla registrazione irrevocabile su Blockchain e l'utilizzo sarebbe regolato da appositi smart contract [21].

CONCLUSIONI

L'obiettivo dal presente rapporto tecnico consiste nel descrivere gli aspetti normativi e tecnologici relativi alla trasmissione e alla gestione delle informazioni nel mondo Internet of Things.

È stato definito il concetto di Internet of Things presente in letteratura analizzando alcuni benefici che questa tecnologia può introdurre per migliorare le condizioni e la qualità della vita degli utilizzatori di tali servizi, cercando contemporaneamente di non dimenticare quelle che sono le problematiche principali da considerare e che mettono a rischio la fattibilità dello sviluppo futuro di tali tecnologie, riguardanti appunto la loro insufficiente sicurezza. Inoltre è molto importante poter anche garantire adeguate strategie di protezione della privacy dei dati. A tale scopo è stata presentata un'architettura suddivisa a livelli che è in grado di implementare adeguate strategie di protezione della privacy basata sui ruoli ricoperti da ciascun livello architetturale.

Sono state analizzate le caratteristiche evolutive delle norme regolamentari dell'IoT, evidenziando le correlazioni presenti tra l'IoT stesso e il regolamento generale sulla protezione dei dati (GDPR), che è diventato operativo da Maggio 2018.

Inerente al GDPR, sono stati descritti ed evidenziati i ruoli e le responsabilità delle entità coinvolte nella raccolta, nell'archiviazione e nel trattamento dei dati personali e sono stati approfonditi i concetti di Accountability e Data Protection, concetti di rilevante importanza affinché possano essere garantiti meccanismi di tutela della privacy e protezione dei dati personali nel mondo dell'IoT.

Infine è stato analizzato il concetto di proprietà intellettuale visto come strumento atto a garantire dei meccanismi di protezione degli oggetti che sono frutto dell'inventiva e dell'ingegno umano. In modo particolare, in ambito IoT, esistono due tipologie di strumenti che possono tutelare la proprietà intellettuale, rappresentate appunto dalle tecnologie Blockchain e Smart Contracts.

BIBLIOGRAFIA

[1] M. Iaselli, S. Gorla “Storia della Privacy”, June 2015.

[2] https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/.

[3] https://ec.europa.eu/digital-single-market/en/news/conclusions-internet-things-public-consultation.

[4] https://www.garanteprivacy.it/documents/10160/10704/1799578.

[5] Chao Li, Balaji Palanisamy, “Privacy in Internet of Things: from Principles to Technologies.”, IEEE Internet of Things Journal, February 2019.

[6] http://www.dirittobancario.it/approfondimenti/fintech/internet-things-e-fintech-evoluzione-normativa-di-una-rivoluzione-tecnologica.

[7] https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en.

[8] https://www.privacy.it/2018/09/04/decreto-legislativo-101-2018/.

[9] https://www.altalex.com/documents/news/2018/04/12/articolo-5-gdpr-principi-trattamento-di-dati-personali.

[10] https://www.garanteprivacy.it/regolamentoue/DPIA;

[11] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

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

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

[14] https://www.linq.it/wp-content/uploads/Decoding_GDPR_Roles_and_Responsibilities.pdf.

[15] J. Singh, C. Millard, C. Reed, J. Cobbe, J. Crowcroft – “Accountability in the Internet of Things (IoT): Systems, law & ways forward”, IEEE Computer Society, July 2018.

[16] https://www.mdpi.com/2624-6511/1/1/6/pdf.

[17] https://clusit.it/rapporto-clusit/ (Anno 2019).

[18] https://www.owasp.org/images/1/1c/OWASP-IoT-Top-10-2018-final.pdf.

[19] https://www.ibanet.org/Article/NewDetail.aspx?ArticleUid=5c133514-208d-4e69-85bb-4a96406d71c0.

[20] https://siac.gdf.it/Eventi/Pagine/IoT-un-opportunit%C3%A0-per-l%E2%80%99Industria-4.0-ed-una-sfida-per-la-tutela-della-propriet%C3%A0-intellettuale.aspx.

[21] http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_IT.pdf.