Politecnico di Torino

Corso di Laurea Magistrale in

Ingegneria Informatica

Tesi di Laurea Magistrale


# Privacy dashboard, sviluppo di una Web App per la gestione del GDPR

**Relatore:**
Prof. Luca Ardito

**Candidato:**
Filippo Peron

Anno accademico 2022/2023

*"Sai,*
*secondo me,*
*Milhouse è*
*el Barto"*
*Homer Simpson*

**Sommario**

Nella presente tesi viene prima presentato e spiegato il GDPR, il regolamento europeo sulla protezione dei dati, per poter discutere del suo impatto, delle sue conseguenze e delle sue attuali limitazioni.

Successivamente viene introdotto l'ambito della Smart Home, focalizzandosi in particolare sulle problematiche e vulnerabilità che lo caratterizzano. Si parlerà inoltre di SIFIS-HOME, un progetto finanziato dal programma europeo Horizon che ha per scopo la creazione di un framework che migliori la resilienza dei dispositivi interconnesi alla smart home.

Infine, viene presentato il mio lavoro: una dashboard integrata nel progetto SIFIS-HOME che permette una migliore interazioni tra gli attori in gioco nell'ambito della smart home (utenti finali, sviluppatori, titolari del trattamento...) e che offre agli utenti un veloce e semplice strumento per applicare i diritti garantiti dal GDPR.

# Indice

# Elenco delle figure

# Capitolo 1

# General Data Protection Regulation

## 1.1 Storia della Privacy

### 1.1.1 Definizione e utilità

Per poter parlare del progetto svolto per questa tesi e del regolamento europeo, il GDPR, a cui si fa riferimento ritengo necessaria una breve discussione sulla storia che ha portato all'adozione di tale testo, enfatizzando in particolare sul ruolo giocato dalla privacy e dalla concezione che se ne ha.

Alan Westin, uno dei pionieri nell'ambito della privacy e i cui lavori vengono diffusamente citati ancora oggi a più di 50 anni di distanza, definisce la privacy come "*la rivendicazione di un individuo, gruppo od organizzazione di determinare da sé quando, come e in che quantità comunicare ad altri delle informazioni che lo riguardano; da un punto di vista relazionale è il volontario e temporaneo distacco di un individuo dalla società in maniera fisica o psicologica, sia in uno stato di solitudine che attraverso l'intimità di un piccolo gruppo*". [1]

Da questa citazione, si possono distinguere nettamente due dimensioni differenti di privacy: una che riguarda il modo in cui un individuo si relaziona con altre persone, ad esempio controllando chi entra in un ambiente domestico o chi ha il

permesso di entrare nel proprio spazio intimo, mentre la seconda riguarda il modo in cui le informazioni personali vengono trattate. Entrambi questi aspetti hanno in comune la necessità di mantenere il controllo dello spazio personale, del corpo e delle informazioni personali di una persona.

Sempre Alan Westin, nel suo libro *Privacy and Freedom*, analizza i motivi per cui la privacy abbia una tale importanza e li sintetizza in quattro funzioni principali:

- **Autonomia personale**: la privacy, impedendo a individui esterni di penetrare nella sfera più intima e personale dell'individuo con la possibilità di influenzarne le idee e scelte, ne protegge l'autonomia e permette il normale sviluppo dell'individualità e dell'indipendenza, qualità fondamentali in special modo nelle società democratiche

- **Scarico emotivo**: la vita in generale crea un livello di stress e di pressione per cui è spesso necessario uno sfogo emotivo, o un rilassamento delle comuni regole sociali. Ciò, tuttavia, è possibile solamente in uno stato di riservatezza in cui non ci si senta osservati o giudicati e ci si possa esprimere in maniera libera e senza blocchi. La mancanza di questi momenti di sfogo e di riservatezza può causare stati di malesere che vanno da un incremento della tensione nervosa a una maggiore tendenza al suicidio

- **Autovalutazione**: il modo che hanno le persone per processare correttamente le informazioni che acquistano costantemente dal mondo esterno è attraverso attimi di riservatezza e solitudine. Solo questi momenti, infatti, permettono a un individuo di integrare correttamente le varie esperienze e di analizzarle in una chiave personale, permettendo anche un'autovalutazione morale dei propri comportamenti

- **Comunicazioni limitate e protette**: la possibilità di avere delle comunicazioni limitate e protette, cioè comunicando solamente ciò che si desidera

esclusivamente con chi si desidera, permette all'individuo di condividere confidenze con persone fidate, cosa possibile solo perché consapevole del fatto che quanto rivelato non sarà condiviso a terzi. Sotto questo punto di vista è di fondamentale importanza la riservatezza imposta ai professionisti, quali medici, psicologi e avvocati. [1]

Al giorno d'oggi il dibattito sulla privacy è particolarmente acceso; la motivazione è senza dubbio da riscontrarsi nella creazione e nell'eccezionale distribuzione delle tecnologie e delle pratiche che hanno il potenziale di invadere la privacy di un individuo. Tuttavia, questo dibattito è tutt'altro che recente, e in modi diversi è stato sviluppato in vari contesti.

### 1.1.2 In pasato nel mondo occidentale

La questione della privacy può essere intravista sin dall'antica Grecia, fu qui infatti che si sviluppò maggiormente la concezione di vita pubblica (o meglio dire politica) come la intendiamo oggi. Aristotele, nella *Politica*, fa una netta distinzione tra sfera privata (Oikos) e sfera politica (Polis) [2]. Per il pensiero greco, infatti, non solo la capacità umana di organizzarsi politicamente è differente, ma è in netto contrasto con i rapporti naturali il cui centro è la casa (Oikiri) e la famiglia. La nascita dell'antica città stato greca, ha significato per il cittadino "ricevere una sorta seconda vita, il suo bios politikos. Ora il cittadino appartiene a due ordini di esistenza e c'è una chiara distinzione tra ciò che è suo (idion) e ciò che è comune (koinon)" [3]

È necessario rimarcare tuttavia che il diritto a questa seconda vita pubblica era riservato solo a una piccola fetta di popolazione, gli uomini liberi. Ciò che distingue maggiormente questi due mondi è infatti il rapporto che c'è tra le persone: il mondo

politico si basava sull'uguaglianza degli individui e sulla libertà [1] mentre il mondo domestico era basato sul dominio totale del capofamiglia (despotes) sia sugli schiavi che sui familiari.
La concezione di privacy per gli antichi greci, ripresa in larga parte anche dai romani, è ancora distante da come la intendiamo noi oggi e, contrapposta alla sfera pubblica e politica, ne assumeva una connotazione principalmente negativa (non è un caso, infatti, che il termine privato derivi dal verbo 'privare', a significare la privazione all'ambiente politico, il solo posto in cui l'uomo è libero). È soltanto in tempi più recenti che questo concetto inizia ad assumere un aspetto positivo e la motivazione va ricercata nel mutamento della concezione della vita pubblica e politica.

Dopo la caduta dell'impero romano e l'inizio del Medioevo, la superiorità dell'aspetto politico su quello privato decade, e sembra quasi essere sostituita dalla superiorità dell'aspetto sacro sulla bassezza della vita quotidiana privata [4]. In questo periodo ciò che nell'antichità apparteneva alla vita privata appartiene ora in larga parte alla vita nel feudo, dove il capofamiglia viene sostituito dal signore feudale e le relazioni interpersonali sono paragonabili più ai rapporti interni delle antiche famiglie rigorosamente gerarchiche che ai rapporti egualitari dei liberi cittadini della polis. In questo nuovo periodo si assiste all'avvento della sfera sociale in cui, per usare le parole di Hannah Arendt, "*l'amministrazione domestica, delle sue attività peculiari, dei suoi problemi e dei suoi strumenti specifici fuoriesce dall'oscura interiorità della casa alla luce della sfera pubblica; ciò ha non solo confuso l'antica demarcazione tra il privato e il politico ma ha anche modificato, fino a renderlo irriconoscibile, il significato dei due termini e la loro importanza per la vita*

[1] per Aristotele uno stile di vita libero doveva essere in totale indipendenza dalle necessità della vita. Tali necessità, principalmente identificabili come 'lavoro', comprendendo sia il lavoro di uno schiavo che quello di un artigiano, appartenevano alla sfera privata. Aristotele distingue tre stili di vita liberi, in cui si abbandona il necessario per concentrarsi su ciò che è 'bello', e uno di essi è appunto interamente dedicato alla vita nella Polis [2]

*dell'individuo e del cittadino*" [4]. È importante notare che nella sfera sociale, che viene a soppiantare quasi completamente la sfera politica, si ha la comparsa del lavoro e della produttività che, sottratte alla dimensione domestica e riproduttiva, col tempo arrivano ad occupare completamente il centro della sfera pubblica [5].

Inizia col tempo a svilupparsi il concetto di società, che farà fiorire i moderni stati-nazioni, che, sempre secondo Hannah Arendt, richiede che i cittadini si comportino come membri di una stessa famiglia, guidati dai medesimi interessi. È qui che si inizia a individuare il concetto di privacy inteso come lo intendiamo oggi, quasi come sinonimo di intimità. Uno dei primi esploratori di questo concetto fu Jean-Jacques Rousseau che "si ribellò non contro l'oppressione dello stato, ma contro l'insostenibile perversione della società e della sua intrusione nelle regioni più interne e intime dell'uomo" [4]. La ribellione di Rousseau, e il concetto moderno di privacy, non è opposta alla sfera pubblica e politica intesa nell'antichità, ma alla sfera sociale, che ha da una parte portato allo scoperto ed esteso le funzioni private dell'individuo e dall'altra ridotto le funzioni politiche tipiche della Polis. Prima di analizzare più a fondo l'idea moderna di privacy, è importante considerare due ulteriori ambiti in cui la distinzione tra pubblico e privato può offrire interessanti spunti: il regno animale e le società (impropriamente) definite primitive.

### 1.1.3 Fuori dal mondo occidentale

#### Mondo animale

Sebbene il concetto moderno di privacy sembri essere un concetto esclusivamente umano, numerosi studi sul comportamento animale e sull'organizzazione sociale suggeriscono che il bisogno umano di riservatezza sia in verità un bisogno universale di ogni specie animale. Virtualmente ogni animale tende a dei periodi di reclusione o di intimità in piccoli gruppi, e ha necessità di uno spazio personale minimo, la cui assenza potrebbe mettere a repentaglio la sua stessa sopravvivenza. Per fare

un esempio, l'etologo John B. Calhoun ha effettuato un esperimento in cui tenendo un gruppo di ratti in un ambiente in cui venivano privati del loro spazio personale, i rituali di corteggiamento, la costruzione delle tane, l'allevamento dei cuccioli e la gerarchia sociale venivano disturbati, portando a un incremento dell'aggressività e a comportamenti sessuali più sadici, nonché ad un aumento delle stesse patologie di cui soffre l'uomo quando si trova in ambienti sovrappopolati: pressione sanguigna alta, disturbi circolatori e del cuore. [6] Questo comportamento non è esclusivo dei ratti ma è generico di ogni specie animale, tanto che è stato coniato il termine di 'fogna del comportamento' (in inglese, behavioral sink): espressione usata per denotare quando una società che, seppur protetta da avversità atmosferiche e potenziali predatori e a cui viene garantita abbondanza di risorse come cibo o acqua, tende ad avere comportamenti anomali tali da farla collassare a causa del sovraffollamento. Come ulteriori esempi, si può riportare l'affermazione del biologo e storico naturale David Attenborough dopo una breve fuga di un gorilla da un zoo in cui afferma che i gorilla danno importanza alla loro privacy [7]; oppure si possono citare le osservazioni sui comportamenti degli animali degli zoo quando ci sono persone che li osservano, che mostrano come in questi casi svariate specie abbiano comportamenti meno socievoli tra di loro, diventino più aggressivi e nel caso degli orangotango si coprano più spesso il volto in proporzione al numero di persone presenti [8].

### Società considerate primitive

Sebbene si sia consapevoli del bisogno di riservatezza come bisogno universale e non solo umano, spesso si è considerato che popoli comunemente denominati 'primitivi' non avessero lo stesso nostro senso della riservatezza, facendo notare come questi popoli vivessero in una comunità totale, priva di qualsiasi sorta di velo, sia psicologico che fisico. Sebbene sia innegabile che diversi popoli abbiano una concezione di riservatezza più o meno marcata, tutti i popoli studiati sinora mostrano dei meccanismi sia individuali che comunitari di privacy, sebbene diversi dai nostri,

che dipendono dalle regole e dai tabù della comunità e in particolare dal modo in cui vivono all'interno delle abitazioni.

Per fare un confronto, a Giava, un'isola indonesiana, gli abitanti vivono in famiglie nucleari (padre, madre e figli non sposati) in piccole case di bambù prive di porte e recinzioni e dai muri molto sottili. In queste abitazioni, qualsiasi persona entra ed esce liberamente in qualsiasi stanza e a qualsiasi orario (con l'eccezione della stanza in cui ci si cambia, in cui rimane visibile sia la parte del corpo sotto le ginocchia sia quella sopra le spalle). Non c'è alcun blocco tra il mondo esterno e il mondo interno della casa, e la privacy casalinga come la conosciamo noi è assente. Tuttavia, non si può dire che la popolazione non ricerchi la propria riservatezza, e visto che non può ricercarla fisicamente lo fa a livello psicologico. Le relazioni sociali tra i giavanesi, anche tra stessi familiari, sono molto controllate e discrete: parlano a voce bassa, nascondono le loro emozioni e hanno un insieme di etichette sociali che non permettono di esprimersi liberamente, creando una sorta di muro psicologico per sostituire la mancanza di un muro fisico.

Sempre nell'arcipelago indonesiano, le persone nell'isola di Bali vivono in famiglie estese patrilineari (da una a una decina di famiglie nucleari che sono legate da relazioni sanguigne tra i padri) in delle case con strette porte e circondate da spesse recinzioni. In queste abitazioni, al contrario di Giava, nessuna persona esterna alla famiglia entra nella casa, ad eccezione di rari casi in cui qualche altro parente o amico viene a visitare, ma sempre sotto invito. In questo ambiente, la casa è a tutti gli effetti una protezione e un riparo dal mondo pubblico e permette di relazionarsi in maniera differente: dentro la casa dei balinesi c'è un forte calore, apertura e spontaneità, mentre quando escono di casa si comportano in maniera più riservata e formale.

Le abitudini differenti di questi due popoli fanno capire i vari modi in cui il bisogno di riservatezza si manifesta in base alle diverse culture: i giavanesi non avendo spazi fisici adibiti alla privacy, compensano con una discrezione sociale incredibilmente

elevata anche all'interno della casa, volta a non manifestare e a tenere privati i sentimenti e le opinioni delle persone; la società balinese invece riconosce la casa come fonte di riservatezza e sicurezza, in cui le persone possono esprimersi liberamente ed essere se stesse senza sentirsi giudicate o sentire l'intromissione di estranei, e questo li porta ad avere comportamenti differenti in casa e fuori di casa; entrambe le popolazioni comunque attuano dei meccanismi per preservare la riservatezza, da una parte a livello fisico, dall'altra a livello psicologico. [9]

### 1.1.4 Ai giorni d'oggi

Dal punto di vista giuridico, l'inizio della moderna discussione riguardante il diritto alla privacy viene fatto risalire ad un saggio scritto da due giuristi statunitensi, Samuel D. Warren II e Louis Brandeis, pubblicato nel 1891 nella rivista accademica *Harvard Law Review*. Nel saggio, nato dalla volontà di difendersi dalle allora moderne tecnologie e dalle mode che permettevano una più assidua interferenza nella vita privata dei cittadini, in particolare la fotografia e il giornalismo scandalistico, i due autori analizzano e descrivono l'evoluzione del principio fondamentale per cui '*un individuo deve avere una protezione completa della sua persona e delle sue proprietà*', affermando che il diritto ad essere lasciati da soli sia indispensabile a tale principio e che le leggi di allora non erano sufficienti a difendere tale diritto. Il saggio ebbe un elevatissima influenza ed importanza, tanto da venir definito come 'probabilmente il più famoso e certamente il più influente articolo di legge mai scritto' [10] e considerato responsabile di 'aver aggiunto un capitolo alla nostra legge [statunitense]' [11]

Per inquadrare opportunamente l'importanza di tale saggio e dei successivi lavori che ha influenzato è necessario sottolineare come nella costituzione degli Stati Uniti, così come in quella di molti altri paesi, tra cui l'Italia, il diritto alla privacy non viene mai esplicitamente affermato. Le motivazioni di tale mancanza sono

principalmente due: innanzitutto si considera il concetto di privacy come innato nello spirito statunitense sin dalle origini e quindi superfluo specificarlo nella costituzione: la colonizzazione dell'America infatti garantì ai cittadini ampi spazi personali permettendo un elevato distanziamento tra le singole case(cosa impossibile nel vecchio continente), accentuando e interiorizzando così il concetto di privacy fisica [12](ancora oggi la densità di popolazione degli Stati Uniti è più di otto volte più bassa rispetto a quella del Regno Unito) [13]; la seconda motivazione è da riscontarsi nel fatto che la reale minaccia alla privacy si è presentata successivamente, con l'avvento dello sviluppo dei media e delle telecomunicazioni.

Tuttavia, un forte impegno giuridico verso la protezione della privacy inizia solo dopo la Seconda Guerra Mondiale, probabilmente come risposta agli abusi perpetuati dai governi fascisti prima e durante la guerra. E' nel 1948 infatti che l'assemblea generale delle Nazioni Unite scrive la 'Dichiarazione Universale dei Diritti dell'Uomo', il cui articolo numero 8 recita così: "*Nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesione del suo onore e della sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge, contro tali interferenze o lesioni*" [14]. Solo due anni dopo, nel 1950 la Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali introduce nell'articolo 8 il Diritto al rispetto della vita privata e familiare che recita così: "*Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui*" [15]. Questi due testi sono fondamentali per l'attuazione di tutele per il rispetto della privacy, in particolar modo per gli stati

nella cui costituzione non c'è un riferimento esplicito a tale diritto, e da allora ci sono state svariate direttive, leggi e regolamenti a riguardo. Si analizzeranno ora le varie misure prese per salvaguardare tale diritto negli Stati Uniti e in Unione Europea, analizzandone lo sviluppo, le analogie e le differenze.

### Stati Uniti

Negli Stati Uniti, i primi sviluppi si fecero grazie alle decisioni della Corte Suprema: nel 1965 la causa 'Griswold v. Connecticut' permise la protezione dei cittadini contro la perquisizione e il sequestro ingiustificati, mentre nel 1966 la causa 'Kats v. United States' estese il Quarto Emendamento, che garantisce il diritto alla sicurezza della persona, includendo ogni area in cui il cittadino ha una 'ragionevole aspettativa alla privacy'. Un altro importante passo avanti fu l'introduzione dal Privacy Act del 1974, redatto nel momento in cui più si sentiva la necessità di una legge che tutelasse i cittadini contro interferenze ingiustificate. Solo 2 anni prima, infatti, ci fu lo scandalo Watergate: il 17 giugno 1972 cinque uomini furono arrestati nel tentativo di inserire delle cimici nei telefoni degli uffici del Comitato Nazionale del partito democratico. Successivamente si scoprì che due di loro erano ex agenti CIA molto vicini all'allora presidente Nixon. Il caso, accanitamente seguito dall'intera popolazione e che portò alle dimissioni del presidente, rese chiare le potenzialità dell'uso di intercettazioni telefoniche e delle cimici spia, rendendo necessaria una legge che ponesse freno a tali abusi [5]. Il Privacy Act fornisce delle regole riguardo la raccolta, l'uso e la distribuzione dei dati personali, impedendone la distribuzione senza consenso scritto ad eccezione di casi particolari [16]. Tale regolamento, tuttavia, ha una valenza solamente nel settore pubblico, e non in quello privato, per timore del potenziale impatto negativo sullo sviluppo dell'iniziativa economica privata; questa scelta, ribadita nei regolamenti successivi, ha segnato una forte spaccatura tra le norme statunitensi e quelle europee, che coinvolgono anche i settori privati [5].

Le azioni a beneficio della protezione della privacy continuarono a prosperare (ad esempio nel 1996 vennero adottate misure per proteggere i dati personali in ambito medicale e di salute [17], mentre nel 1998 le misure furono a favore della protezione dei minori di 13 anni [18]), fino a un'inversione di tendenza causata dall'attacco terroristico dell'11 settembre 2001. Neanche un mese dopo l'attentato, il Congresso approvava il Patriot Act: una serie di provvedimenti tesi ad aumentare i poteri della polizia in vari campi, particolarmente in quello del controllo delle comunicazioni. L'attentato non ebbe ripercussioni solo sugli Stati Uniti ma anche su molte altre nazioni occidentali, favorendo in special modo l'introduzione di nuovi sistemi di identificazione dei cittadini. Già un anno dopo l'attentato, l'associazione "Reporters sans frontiéres" denunciava i cambiamenti in atto in ambito di sorveglianza e libertà individuali, descrivendo come, sotto l'egida della guerra al terrorismo, i controlli su Internet e altri mezzi di comunicazione elettronica fossero aumentati in maniera esponenziale. Alcune delle democrazie occidentali sono state descritte dall'associazione come "predatori di libertà digitali". Nel rapporto, diffuso nella sede dell'associazione a Parigi, si legge tra l'altro: "Ad un anno dai tragici eventi di New York e Washington, Internet può essere inclusa nell'elenco dei "danni collaterali". Le cyber-libertà sono state minacciate e le fondamentali libertà digitali amputate". La situazione da allora è rimasta pressoché immutata.

### Italia e Unione Europea

Come già anticipato, in Europa il punto di inizio della discussione per il diritto alla privacy è da considerarsi l'articolo 8 della *Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali* del 1950. Da allora, ogni stato ha avuto una notevole autonomia per implementare tale principio, almeno fino alla formale istituzione dell'Unione Europea avvenuta col trattato di Maastricht del 1992.

In questo periodo in Italia ci furono alcuni importanti sviluppi: inizialmente non

si ammetteva il diritto alla riservatezza, la costituzione italiana infatti non include esplicitamente tale diritto, ed era considerato come incluso nel più ampio diritto alla personalità. Negli anni ci furono vari casi giuridici in cui si cercò di invocare tale diritto e che permisero di compiere dei passi in avanti decisivi per il suo riconoscimento; uno dei casi più importanti fu il caso del settimanale "Il Tempo" che, in una serie di articoli, pubblicò diversi particolari della vita intima di Claretta Petacci, l'amante di Benito Mussolini. I familiari della Petacci, ritenendo le descrizioni del giornale offensive gli fecero causa, vincendo appellandosi alla Corte di Costituzione che emise una decisiva sentenza che mutava la rigida posizione iniziale sul tema: "Sebbene non sia ammissibile il diritto tipico alla riservatezza, viola il diritto assoluto di personalità, inteso quale diritto erga omnes alla libertà di autodeterminazione nello svolgimento della personalità dell'uomo come singolo, la divulgazione di notizie relative alla vita privata, in assenza di un consenso almeno implicito, ed ove non sussista, per la natura dell'attività svolta dalla persona e del fatto divulgato, un preminente interesse pubblico di conoscenza". [5]. Nel nostro paese non ci furono cambiamenti decisivi nell'orientamento giurisprudenziale fino al 1973, anno in cui la Corte Costituzionale afferma che, seppur non esplicitato nella costituzione italiana, il diritto alla riservatezza è affine e a sostegno degli articoli 2 e 15 della costituzione italiana e degli articoli 8 e 10 della Convenzione Europea dei diritti umani [19]

Intanto, nel 1981 esce un documento fondamentale, il testo dell'OCSE (Organizzazione per la cooperazione e lo sviluppo economico) dove vengono proposti sette principi base per una corretta politica della protezione dei dati personali, riassunti qui sotto:

- **Notifica**: le persone devono essere avvisate nel momento in cui vengono raccolti i loro dati
- **Scopo**: i dati devono essere usati solo per lo scopo specificato e non per altri
- **Consenso**: i dati non devono essere divulgati senza il consenso della persona

- **Sicurezza**: i dati devono essere tenuti in sicurezza da possibili abusi
- **Conoscenza**: la persona dev'essere a conoscenza di chi sta collezionando i suoi dati
- **Accesso**: la persona deve avere la possibilità di accedere ai propri dati e correggere qualsiasi inesattezza
- **Responsabilità**: dev'esserci un metodo per rendere responsabile chi mantiene i dati nel caso non rispetti tali principi [20]

Queste raccomandazioni vennero pressoché ignorate nel territorio statunitense mentre ebbero una fortissima influenza in ambito europeo. Una decina d'anni dopo, infatti, successivamente al trattato di Maastricht del 1992, escono in Unione Europea varie direttive in materia di protezione dei dati in cui tali principi vengono ripresi e ampliati. Va specificato che, in quanto direttive, non avevano potere di norme per gli stati membri: ogni stato infatti doveva provvedere alla creazione di specifiche leggi per rispettare ciascuna normativa. La prima è del 1995, la direttiva 95/46/Ce comunemente chiamata 'Data Protection Directive', "*relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*" [21], seguita nel 1997 dalla direttiva 97/66/Ce, "*sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni*" [22] e infine la direttiva del 2002, la 2002/58/Ce, "*relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche*" [23].
In particolare, nella direttiva del 1995, si precisa che i dati devono essere, tra l'altro, trattati lealmente e lecitamente; rilevati e trattati per finalità determinate, esplicite e legittime; adeguati, pertinenti e confacenti alle suddette finalità; esatti e, se necessario, aggiornati. Inoltre, la persona i cui dati sono oggetto di trattamento ha tutta una serie di diritti che vanno dal diritto di accesso ai dati medesimi (art. 12, Direttiva 95/46/CE), al diritto alla rettifica o alla rimozione, nonché un diritto

di opposizione. Per di più, la Direttiva dispone il divieto per i Paesi membri di trattare dati particolari che rivelino l'origine razziale o etnica, le idee politiche, le convinzioni religiose o filosofiche [24].
Tale direttiva, che in Italia determinò l'adozione della legge 675/1995 e che istituì la figura del Garante per la protezione dei dati personali, venne sostituita nel 2016 dal Regolamento generale sulla protezione dei dati (o in inglese General Data Protection Regulation, GDPR), che verrà analizzato nel dettaglio nella prossima sessione.

## 1.2 GDPR

Il regolamento generale sulla protezione dei dati (in inglese General Data Protection Regulation, GDPR) ufficialmente regolamento (UE) n. 2016/679, è un regolamento dell'Unione europea relativo alla privacy e al trattamento dei dati personali. È stato adottato il 27 aprile 2016, mentre la sua pubblicazione sulla Gazzetta ufficiale dell'Unione europea risale al 4 maggio 2016, è entrato in vigore il 24 maggio dello stesso anno ed è operativo a partire dal 25 maggio 2018. In quanto regolamento, e non direttiva, è direttamente applicabile e considerato come norma per i singoli stati dell'Unione, senza necessità di creare apposite leggi.
Come riassunto in *Figura* 1.1, la nascita di questo testo è da ricercarsi già nel 2012: il 25 gennaio di quell'anno infatti la Commissione Europea propose una riforma alla direttiva del 1995, al fine di aumentare i diritti alla privacy online e dare una spinta maggiore all'economia digitale europea; il 12 marzo 2014 il Parlamento Europeo dà supporto alla riforma con 621 voti favorevoli, 10 contrari e 22 astenuti mentre il 15 dicembre 2015 si raggiunge un accordo tra il Consiglio dell'Unione Europea, il Parlamento Europeo e la Commissione Europea che portò alla definitiva stesura del testo nel 2016.
Il regolamento, composto da 99 articoli suddivisi in 11 capitoli a loro volta divisi

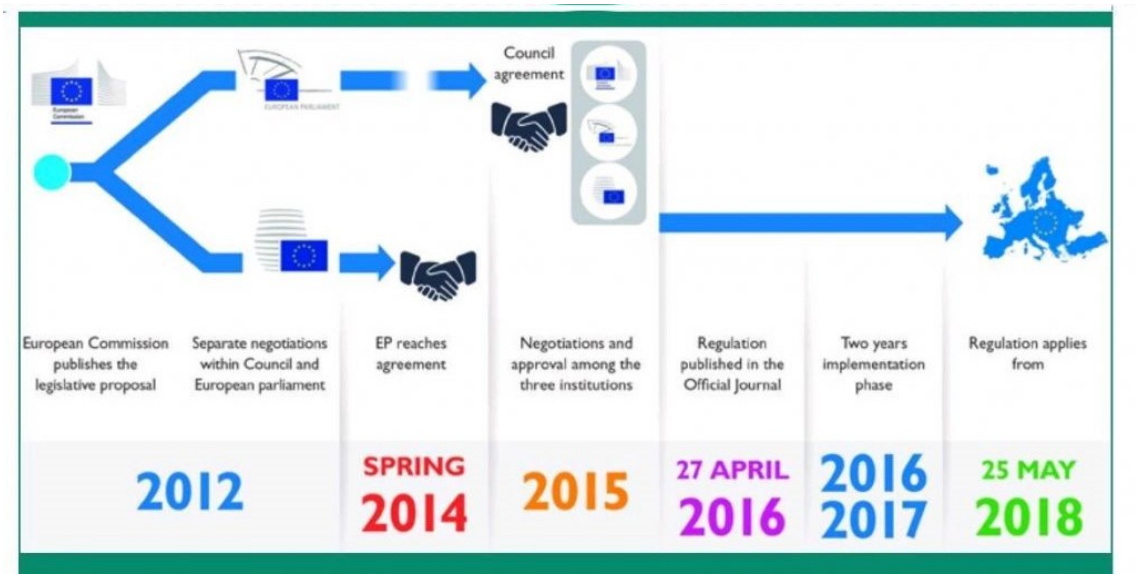



Figura 1.1: Storia della nascita del GDPR.

in varie sezioni, ricopre una vasta area di influenza. Uno dei suoi punti di forza maggiori infatti deriva dal fatto che il regolamento non deve essere rispettato solamente da società con sede in Unione Europea, ma da chiunque tratti dati personali di un cittadino dell'Unione Europea. Ad esempio, se un cittadino spagnolo utilizza un'applicazione statunitense come Whatsapp, i suoi dati personali dovranno essere trattati secondo le norme del GDPR, sebbene l'azienda non sia sul territorio europeo.

### 1.2.1 Concetti base

#### Obiettivo

L'obiettivo del regolamento, come specificato nell'articolo 1 comma 1 *Oggetto e finalità* è quello di "*stabilire norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati*". Con questa affermazione si intende specificare e distinguere le due finalità principali del testo: la prima è la protezione delle persone fisiche e dei

loro dati personali mentre la seconda è la libera circolazione di tali dati. La prima finalità, ribadita nel secondo comma dello stesso articolo che afferma la volontà di "*proteggere i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali*", viene chiarita ed elaborata dettagliatamente nel contenuto degli articoli successivi. Per comprendere appieno la seconda finalità invece, bisogna considerare il forte impegno dell'Unione nella libera circolazione di persone e merci all'interno del suo territorio; questo regolamento vuole quindi ampliare tali categorie per includere anche i dati personali, continuando nell'impegno dell'Unione a consolidare un mercato unico digitale. Questo principio di libero scambio dei dati è considerato altamente prioritario, come si può evincere dal comma 3 del primo articolo: "*La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali*".

### Definizioni chiave

Il GDPR introduce alcuni termini, fondamentali soprattutto per la corretta comprensione degli attori in gioco, e di seguito vengono elencati i più importanti:

- **Dati personali**: qualsiasi informazione che abbia una relazione con un individuo che può essere direttamente o indirettamente identificato. Nomi e indirizzi mail sono esempi di dati personali così come le informazioni di localizzazione e i web cookies. Anche i dati pseudonomizzati, in caso sia facilmente possibile identificare la persona, sono considerati dati personali. Tra i dati personali è presente la così detta categoria particolare di dati personali: cioè i dati che permettono di rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, biometrici e relativi alla salute, vita sessuale e all'orientamento sessuale dell'individuo

- **Processamento dei dati**: qualsiasi azione effettuata sui dati peronsali, sia automatica che manuale. Come titolo di esempio, le seguenti azioni sono considerate come processamento di dati: collezionare i dati, salvare i dati, eliminare i dati, organizzare i dati
- **Interessato (Data Subject)**: la persona i cui dati vengono processati
- **Titolare del trattamento (Data Controller)**: la persona che decide come e perché i dati vengano processati
- **Responsabile del trattamento (Data Processor)**: una persona terza che processa i dati personali al posto del data controller. A titolo di esempio, vengono considerati responsabili del trattamento i servizi cloud e i servizi di posta elettronica.

### DPO

Un'altra importante novità introdotta dal GDPR è la creazione del ruolo di Responsabile della Protezione dei Dati, o Data Processor Officer (DPO). Questa figura, designata dal titolare del trattamento e dal responsabile del trattamento, è obbligatoria solo in specifici casi, ossia quando l'organizzazione che tratta i dati rientra in una di queste tre casistiche:

1. il trattamento viene effettuato da un'autorità pubblica, ad eccezione di autorità giurisdizionali;
2. le attività principali dell'organizzazione consistono in trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
3. le attività principali dell'organizzazione consistono nel trattamento, su larga scala, di categorie particolari di dati personali

Solo in questi casi quindi si richiede la figura del DPO, un soggetto interno o esterno all'organizzazione, con specifiche competenze giuridiche, informatiche e relative all'analisi dei rischi e dei processi, il cui compito è osservare, valutare e organizzare

la gestione del trattamento dei dati personali, nonché di verificare il rispetto delle norme della privacy e di interfacciarsi con le autorità competenti e i titolari dei dati.
Viene inoltre sottolineato come il DPO non debba ricevere alcuna istruzione per quanto riguarda l'esecuzione dei suoi compiti, come debba essere sostenuto appieno fornendogli le risorse necessarie ad assolvere ai propri compiti e come debba riferire esclusivamente e direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento. In questo modo si garantisce che non solo il DPO abbia una gamma di responsabilità molto ampia, ma anche che sia protetto da potenziali interferenze da parte dell'organizzazione.

### Privacy Notice

Il Privacy Notice o Privacy Policy è un importantissimo documento pubblico che permette agli utenti di effettuare delle scelte informate riguardo ai loro dati personali. Questo documento infatti spiega come un'organizzazione processa i dati personali e come applica i principi della protezione dei dati. Gli articoli 12, 13 e 14 forniscono dettagliate istruzioni per la creazione del documento, e in particolare viene specificato che esso dev'essere conciso, trasparente, facilmente accessibile, scritto in un linguaggio semplice e chiaro e gratuito.
Le informazioni che devono essere contenute sono le seguenti:

1. l'identità e i contatti dell'organizzazione e dei suoi rappresentanti
2. lo scopo del processamento e le sue basi legali
3. i dettagli riguardanti qualsiasi trasferimento dei dati a paesi terzi
4. il periodo di mantenimento dei dati
5. l'esistenza dei diritti che possiedono i Data Subjects
6. l'esistenza di sistemi di decisione automatizzati

### 1.2.2 Principi del GDPR

#### Principi base

Sebbene il testo sia molto ampio e gli ambiti di applicazione numerosi così come le regole introdotte, sono presenti sette principi base del GDPR che ne riassumono la filosofia. Questi principi, definiti all'articolo 5, *Principi applicabili al trattamento di dati personali*, vengono riassunti qui sotto.

- **Liceità, correttezza e trasparenza**: i dati devono essere processati in maniera lecita, corretta e trasparente nei confronti dell'interessato. Ciò significa che, nel processamento dei dati, non deve venire infranta nessun'altra legge e i proprietari dei dati (Data Subjects) devono essere informati e sentirsi trattati in maniera onesta.
- **Limitazione della finalità**: i dati devono essere raccolti per finalità determinate, esplicite e legittime. I dati devono essere processati in maniera che non ci sia incompatibilità con tali finalità. Ciò vuol dire che le richieste di consenso non devono essere generali (finalità esplicite) e che trattamenti che esulino dalle finalità dichiarate non sono ammissibili
- **Minimizzazione dei dati**: i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità. È necessario dunque collezionare la minor quantità possibile di dati, e solo se assolutamente necessario agli scopi dichiarati
- **Esattezza**: i dati devono essere esatti e, se necessario, devono essere opportunamente aggiornati. Devono inoltre esserci tutte le misure ragionevoli per cancellare o rettificare in maniera tempestiva i dati inesatti
- **Limitazione nella conservazione**: i dati non devono essere conservati per un periodo di tempo maggiore dello stretto necessario per la finalità dichiarata. Dev'esserci quindi una cancellazione periodica dei dati più vecchi e nessun dato può essere memorizzato senza limitazione di tempo

- **Integrità e riservatezza**: i dati devono essere trattati in maniera da garantire un'adeguata sicurezza, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali
- **Responsabilizzazione**: il responsabile del trattamento è ritenuto responsabile delle misure prese e dev'essere in grado di dimostrare il rispetto di tutti i precedenti principi. Uno dei modi consigliati per provare il rispetto dei principi è di possedere una dettagliata ed esplicita documentazione dei dati collezionati, di come sono utilizzati, salvati e chi sono i responsabili dei dati

### Protezione e sicurezza

Il regolamento prevede che siano presenti appropriate misure tecniche e amministrative che garantiscano opportuni livelli per un sicuro processamento dei dati. Tra queste misure, l'articolo 32 cita la cifratura dei dati personali, la garanzia di confidenzialità e integrità, la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico e l'utilizzo di una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
Viene inoltre specificato come in caso di Data Breach (un incidente di sicurezza, durante il quale i dati sensibili degli utenti vengono consultati, copiati, rubati o trasmessi da soggetti non autorizzati) si è tenuti ad avvisare l'autorità competente entro 72 ore e di informare i titolari dei dati nei casi in cui la violazione sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.
Sono anche riportate delle misure tipo che le aziende possono adottare per avere un livello di sicurezza adeguato: tra queste ci sono l'effettuare la pseudonimizzazione dei dati il prima possibile, permettere al titolare dei dati di monitorare il processamento dei dati e permettere al titolare del trattamento di creare e migliorare le caratteristiche relative alla sicurezza.

Inoltre, l'articolo 25 specifica che tutti i servizi e processi che usano dati personali devono essere progettati per proteggere tali dati in tutte le fasi di progettazione ed implementazione (principio di privacy by design e by default) e i responsabili devono essere in grado di dimostrare che i dati sono protetti con misure adeguate e che i principi di rispetto della privacy sono applicati e verificati in maniera continua. Questo principio di privacy by design e by default, introdotto già prima del GDPR da Ann Cavoukian, ex commissario della privacy dell'Ontario, ha al suo interno altri 7 principi fondamentali [25]. Vista l'importanza primaria di tale principio nella filosofia stessa del GDPR, questi principi, riassunti in *Figura* 1.2 saranno ora brevemente descritti:

- **Proattivo non reattivo**: è importante prevenire possibili violazioni relative alla privacy prima che accadano effettivamente. L'implementazione del principio di privacy by design implica che non bisogna aspettare che il rischio si materializzi, né offrire un rimedio per risolvere un'avvenuta infrazione, l'obiettivo deve invece essere impedire possibili infrazioni prima che avvengano
- **Privacy come impostazione di default**: questo principio garantisce che la privacy sia implementata di default nella maniera più stringente possibile; se un utente non fa alcuna richiesta, devono essere comunque impostati i criteri più stringenti per la protezione dei dati
- **Privacy incorporata nella progettazione**: la privacy deve diventare una componente essenziale del prodotto e dev'essere integrata ad esso sin dal design e non può essere intesa come add-on da implementare successivamente. La privacy diventa parte integrante del sistema senza diminuirne le funzionalità
- **Massima funzionalità**: con questo principio si elimina una spesso diffusa falsa credenza riguardo gli inevitabili compromessi tra privacy e sicurezza o privacy e user experience, in cui si afferma che l'aumento di attenzione in uno di questi aspetti ne danneggi l'altro. La corretta implementazione dei controlli

relativi alla privacy deve invece dare benefici all'intero sistema, dimostrando che è possibile avere entrambi questi aspetti spesso visti in contrasto tra loro. Inoltre, è fondamentale che non ci siano limitazioni delle funzionalità del prodotto per avere un maggiore privacy

- **Sicurezza fino alla fine**: secondo il concetto di Privacy by Design la sicurezza dei dati dev'essere implementata per l'intero ciclo di vita dei dati, fin dal momento in cui si inizia a collezionarli, elaborarli e memorizzarli fino alla loro cancellazione. Questo principio aumenta la sicurezza complessiva del sistema andando a minimizzare i punti critici del sistema
- **Visibilità e trasparenza**: il concetto base di questo principio può essere riassunto con la frase "fidati ma verifica". Questo principio infatti spinge sull'implementazione di soluzioni trasparenti, facilmente visionabili da chiunque e quindi permettendo la facile verifica del prodotto da certificatori o controllori terzi. Questo principio non solo permette un più facile controllo sull'applicazione del regolamento, ma aumenta anche la fiducia dell'utente, in quanto quest'ultimo ha la possibilità di controllare il prodotto che usa
- **Rispetto per la privacy dell'utente**: questo è il principio fondamentale non solo del concetto di Privacy By Design ma dello stesso GDPR. Secondo questo principio l'utente e i suoi dati sono posti al centro del sistema, facendo della privacy dell'utente la preoccupazione principale nello sviluppo di un prodotto. Tale principio si traduce in implementare correttamente tutte le fasi della gestione della privacy e adottare soluzioni forti, rispondere prontamente ai problemi, informare in maniera chiara e utilizzare opzioni user-friendly

### Consenso

Il regolamento si pone l'obiettivo di salvaguardare i dati personali e di dare importanza centrale al titolare di tali dati. Risulta quindi fondamentale in questo

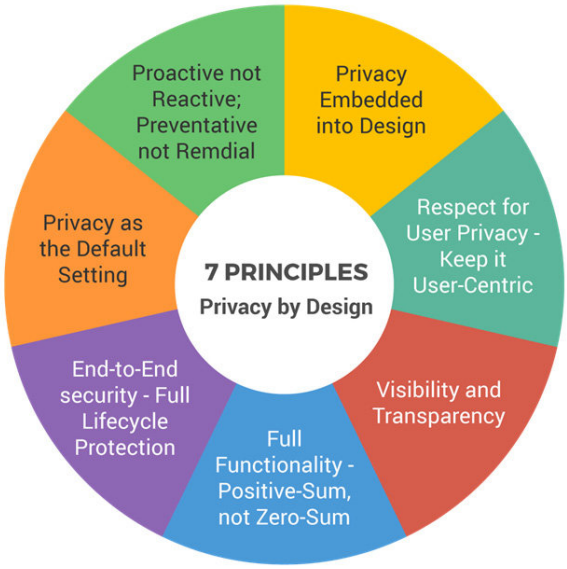



Figura 1.2: Privacy by Design e by Default

contesto dare il pieno e totale controllo all'utente sulla gestione dei suoi dati, facendo in modo che possa decidere autonomamente e liberamente del loro utilizzo. Per questo motivo si è posta una particolare importanza e si sono imposti stringenti limitazioni sul concetto di consenso, il metodo più utilizzato per avere il diritto di processare i dati delle persone, a partire dalla sua definizione presente all'articolo 4, "*consenso: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento*".

Affinché possa essere considerato consenso, quindi, l'interessato deve avere pieno controllo, senza alcuna forma di pregiudizio, di poter scegliere se accettare o meno i termini proposti, senza alcun tipo di ripercussione. Al momento di proporre un trattamento basato sul consenso, il titolare deve fare in modo che vengano rispettate alcune caratteristiche:

- **inequivocabile**: l'interessato deve comunicare il proprio consenso in modo

che non ci sia alcun dubbio sulle sue intenzioni. Ad esempio, azioni come sfogliare la pagina e scorrere un sito, oppure elementi come form precompilati e caselle già spuntate, non soddisfano questa condizione in quanto il comportamento dell'interessato non dimostra una chiara intenzione di consenso alle condizioni

- **liberamente fornito**: l'interessato deve essere in grado di operare una scelta effettiva e non deve subire alcuna intimidazioni o inganno. In caso non venga dato il consenso, l'interessato non deve subire alcuna conseguenza negativa. A titolo d'esempio, azioni come negare la piena funzionalità di un prodotto in caso di mancanza di un consenso, oppure ambiti in cui ci sono squilibri di potere, come casi in cui sia il datore di lavoro a chiedere il consenso ai suoi dipendenti, non soddisfano questa condizione
- **specifico**: ogni consenso deve essere specifico alla finalità per il quale è eseguito il trattamento. Un esempio classico di questa condizione è il consenso dei cookie: per cookies con finalità differenti non può esserci un unico consenso, ma ce ne dev'essere uno per ogni finalità
- **informato**: l'interessato deve essere opportunamente informato dei modi in cui vengono trattati i suoi dati, nonché della finalità del trattamento. Inoltre, l'interessato deve essere pienamente consapevole delle conseguenze del consenso
- **verificabile**: è necessario che il reponsabile del trattamento sia in grado di dimostrare l'avvenuto consenso da parte dell'interessato allo specifico trattamento per l'intero periodo in cui avverrà tale operazione
- **revocabile**: l'interessato deve avere la possibilità di revocare il consenso in qualsiasi momento e in maniera tanto semplice quanto lo è stato darlo. L'interessato non ha alcuna obbligazione a fornire i motivi di tale revoca e il trattamento dovrà interrompersi non appena sarà stato richiesto [26]

L'articolo 7 specifica le disposizioni messe in atto per salvaguardare questa presa di posizione sul consenso e sono le seguenti:

1. la richiesta di consenso deve essere presentata in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro
2. il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali
3. l'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. Il consenso deve essere revocato con la stessa facilità con cui è accordato.
4. nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.

### 1.2.3 Diritti e doveri

#### Diritti dell'interessato(Data Subject)

Il GDPR introduce a favore dell'interessato una serie di diritti, specificati negli articoli dal 15 al 23, che hanno l'obiettivo di fornire più controllo sui suoi dati personali, e sono ora brevemente riassunti:

- **Diritto d'accesso**: l'interessato ha il diritto di ottenere l'accesso ai suoi dati personali, ricevere una copia di questi dati e di ottenere le seguenti informazioni:
  - le finalità del trattamento
  - le categorie di dati personali in questione
  - i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati

  - il periodo di conservazione dei dati personali
  - qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine
  - l'esistenza di un processo decisionale automatizzato, compresa la profilazione, e informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

- **Diritto di rettifica**: L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. In base alle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti.
- **Diritto di cancellazione (diritto all'oblio)**: L'interessato, salvo specifici motivi di sicurezza, di interesse pubblico o altre motivazioni legittime, ha il diritto di ottenere dal titolare la cancellazione dei dati che lo riguardano senza ingiustificato ritardo se sussiste almeno uno dei seguenti motivi:
  - i dati trattati non sono più necessari alle finalità del trattamento
  - l'interessato revoca il consenso al trattamento precedentemente dato
  - l'interessato si oppone al trattamento (vedi sotto, 'diritto di opposizione')
  - i dati personali sono stati trattati illecitamente
  - i dati personali devono essere cancellati per adempiere un obbligo legale
- **Diritto di limitazione di trattamento**: L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento nei casi in cui i dati il titolare ne contesta l'esattezza, il trattamento è illecito oppure l'interessato si sia opposto al trattamento (vedi sotto, 'diritto di opposizione')
- **Diritto alla portabilità dei dati**: L'interessato ha il diritto di ricevere i dati personali che lo riguardano precedentemente forniti a un titolare del trattamento e ha il diritto di trasmettere liberamente e senza impedimenti tali dati a un altro titolare del trattamento

- **Diritto di opposizione**: L'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano e il titolare del trattamento, salvo casi di sicurezza, di interesse pubblico o di altre motivazioni legittime, deve astenersi dal trattare ulteriormente i dati personali
- **Diritti relativo a processi automatici e alla profilazione**: L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.
- **Diritto di reclamo**: l'interessato ha il diritto di proporre un reclamo all'autorità competente

### Doveri del titolare del trattamento (Data Controller/Processor)

Uno dei principi base del GDPR è la responsabilizzazione dei titolari del trattamento dei dati e questi sono quindi soggetti a vari obblighi, descritti negli articoli dal 12 al 14 e dal 24 al 39, e ora brevemente riassunti:

- **Informazioni da fornire all'interessato**: Nel momento in cui vengono acquisiti dei dati personali dell'interessato, il titolare del trattamento deve fornirgli le seguenti informazioni:
  - l'identità e i dati di contatto del titolare del trattamento e del responsabile della protezione dei dati, se presente
  - le finalità del trattamento cui sono destinati i dati personali e in specifiche situazioni i legittimi interessi perseguiti dal titolare del trattamento
  - gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
  - l'eventuale intenzione del titolare del trattamento di trasferire dati personali a un paese terzo

  - il periodo di conservazione dei dati personali
  - l'esistenza dei diritti del titolare dei dati
  - l'esistenza di un processo decisionale automatizzato,

  Questo dovere è alla base della creazione del Privacy Notice, un documento facilmente accessibile dall'interessato in cui sono presenti tutte le precedenti informazioni

- **Facilitare i diritti dell'interessato**: Il titolare del trattamento deve prendere le appropriate misure per facilitare l'esercizio dei diritti dell'interessato e per fornire le informazioni richieste dall'interessato in maniera chiara, concisa, trasparente e facilmente accessibile
- **Protezione dei dati**: Il titolare deve mettere in atto misure tecniche e organizzative adeguate volte ad attuare in modo efficace i principi di protezione dei dati e volte a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento (principio di privacy by design e by default)
- **Sicurezza del processo**: Il titolare deve mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio. Inoltre, in caso di violazione dei dati personali, deve notificare senza ingiustificato ritardo tale violazione all'autorità di controllo competente e, in caso la violazione presenti un rischio elevato per i diritti e le libertà delle persone fisiche, deve avvisare anche quest'ultime descrivendo con un linguaggio semplice e chiaro la natura della violazione dei dati
- **Valutazione d'impatto (Privacy Impact Assessment)**: Nei casi in cui il trattamento dei dati personali può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento deve effettuare, prima di procedere al trattamento, una valutazione dell'impatto. In particolare, i casi in cui sia necessario fare tale valutazione sono i seguenti:

- ci sia una valutazione basata su un trattamento automatizzato e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche
- ci sia un trattamento su larga scala di categorie particolari di dati personali
- ci sia una sorveglianza sistematica 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; 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

### 1.2.4 Impatto GDPR

#### Sanzioni

Il GDPR è ormai in vigore da quattro anni e la sua influenza è ormai accertata e visibile in vari ambiti. Sebbene probabilmente gli utenti medi non abbiano percepito particolari cambiamenti, se non l'onnipresente sezione che compare in ogni sito web visitato e che chiede il consenso all'utilizzo dei cookie, il regolamento ha certamente fornito uno strumento utile a combattere per via giuridica l'abuso dell'utilizzo dei dati personali da parte delle aziende. Nel corso di questi anni infatti sono state numerose le cause intentate per violazioni del regolamento, che hanno comportato anche multe molto salate (il testo prevede infatti sanzioni o fino al 4% del fatturato o fino a 20 milioni euro, si prende il valore più elevato dei due). Le organizzazioni colpite dalle sanzioni sono sia private che pubbliche, tra quest'ultime ricordiamo il caso bonus covid in cui l'INPS (Istituto Nazionale della Previdenza Sociale) ha ricevuto una sanzione da 300mila euro da parte del garante della privacy italiano per "*mancata definizione dei criteri per trattare i dati di determinate categorie di*

*richiedenti il "bonus Covid", uso di informazioni non necessarie rispetto alle finalità di controllo, ricorso a dati non corretti o incompleti, inadeguata valutazione dei rischi per la privacy*" [27].

Tra le dispute legali relative alle società private le più importanti sono la causa vinta dalla Francia contro Google, per una multa complessiva di 50 milioni di euro, per aver mostrato insufficiente controllo, trasparenza e sistema di consenso riguardo l'uso di dati personali utilizzati per pubblicità mirata [28], e la causa intentata dall'Irlanda contro Whatsapp, vinta dalla prima e finalizzata da una sanzione di 225 milioni di euro, con la motivazione di mancata trasparenza riguardo al processamento dei dati [29]. Infine, di grossa importanza è quella che al momento è la sanzione più salata causata dal GDPR: la causa intentata dal Lussemburgo contro Amazon, costata a quest'ultima 764 milioni, per il modo in cui fa pubblicità mirata [30].

### Trasferimento dati fuori dall'UE

Tra le conseguenze più impattanti del GDPR c'è senza dubbio la rivalutazione della liceità del trasferimento dei dati personali verso un paese terzo esterno all'Unione Europea. Dopo l'introduzione del regolamento, infatti, ci sono regole più stringenti in merito alla circolazione dei dati, in particolare gli articoli dal 44 al 50 specificano che sono consentiti trasferimenti di dati a paesi esterni all'Unione Europea solo se sussiste almeno una delle seguenti condizioni:

- la Commissione ha deciso che il paese in cui verranno inviati i dati garantisce un livello di protezione adeguato. Tra gli elementi considerati per valutare tale garanzia vengono citati lo stato di diritto, il rispetto dei diritti umani e delle libertà fondamentali del paese, l'esistenza e l'effettivo funzionamento di una o più autorità di controllo indipendenti e gli impegni internazionali assunti dal paese. Tra le nazioni che hanno ricevuto questa approvazione ci sono il Canada, il Giappone, il Regno Unito e altre.

- il titolare o il responsabile del trattamento ha fornito garanzie adeguate. Come esempi di queste garanzie vengono citati gli strumenti giuridicamente vincolanti, le clausole tipo di protezione dei dati adottate dalla Commissione, un codice di condotta approvato e un meccanismo di certificazione approvato.

- è presente un accordo internazionale tra il paese terzo e l'Unione, o uno stato aderente all'Unione.

- l'interessato ha esplicitamente acconsentito al trasferimento proposto, dopo essere stato informato dei possibili rischi di siffatti trasferimenti

Con tali regole il trasferimento dei dati personali diventa molto più difficile e gli stati non membri dell'Unione Europea devono impegnarsi a rispettarle per poter continuare a ricevere i benefici di un libero scambio di dati. A tal proposito è interessante considerare la politica di scambi avvenuta tra l'Unione Europea e gli Stati Uniti. Il primo accordo avvenuto tra i due organismi risale al 2000, ed è il cosiddetto "International Safe Harbor Privacy Principles" che prevedeva la possibilità di scambio se le aziende statunitensi rispettavano i 7 principi emanati dall'OCSE, discussi nella precedente sezione. Negli anni a seguire tuttavia, diversi report dell'Unione europea verificarono e testimoniarono la mancanza di trasparenza e di rispetto delle norme da parte delle aziende statunitensi, culminata infine con la sentenza Schrems in cui l'attivista austriaco Maximilian Schrems presentò denuncia verso Facebook per violazione della privacy, in seguito alle rivelazioni sulla sorveglianza di massa emesse da Edward Snowden nel 2013 [31] e che portò alla sua invalidità definitiva. Per sostituire questo accordo, nel 2016 venne istituito il Privacy Shield che secondo alcuni avrebbe offerto considerevoli miglioramenti rispetto alla precedente soluzione ma non avrebbe risolto tre problemi fondamentali: la cancellazione di dati, la quantità significativa di dati raccolti e l'assenza di garanti [32]. Tuttavia, questo testo ebbe vita corta, e la sua invalidità è stata proprio causata dal GDPR. Sempre Maximilian Schrems infatti, poco dopo l'attivazione del nuovo regolamento,

fece causa a Facebook per non rispettare il testo in quanto i dati raccolti dall'azienda potrebbero essere resi accessibili dalle agenzie di intelligence statunitensi[2], e per questo motivo nel 2020 la Corte Europea di Giustizia ha invalidato l'accordo [34]. Da allora non è stato ancora approvato alcun accordo ufficiale a sostituire il Privacy Shield anche se si stanno facendo dei negoziati per farne approvare uno nuovo chiamato Trans-Atlantic Data Privacy Framework, rispettoso dei principi del GDPR.

[2]Negli Stati Uniti infatti è presente il cosiddetto Cloud Act che conferisce al governo statunitense di ispezionare qualsiasi dato al di fuori del territorio statunitense [33]

# Capitolo 2

# Internet Of Things

## 2.1 Cos'è

Il progetto svolto rientra nell'ambito dell'Internet delle cose (Internet of Things, IoT, in inglese) e in particolare nella categoria della Smart Home, o domotica in italiano. In questa sezione si andrà ad analizzare questo ambito, focalizzandosi poi sui possibili rischi sulla sicurezza e sulla privacy.

### 2.1.1 Definizione

Sebbene non ci sia un'unica definizione universalmente accettata di Internet Of Things, e anzi spesso viene descritto in maniera differente in base alle caratteristiche e agli attributi più importanti relativi a un certo contesto[1], tutte le definizioni descrivono uno scenario in cui la connettività e la capacità computazionale vengono

[1]L'Internet Architecture Board (IAB) lo definisce come "*un trend dove un grande numero di dispositivi utilizzano servizi di comunicazione offerti dai protocolli internet*" [35], mentre l'International Telecommunication Union (ITU) lo descrive senza neanche fare riferimento a Internet: "*un'infrastruttura globale per la società dell'informazione, che permette dei servizi avanzati interconnettendo oggetti (fisici e virtuali) basandosi su tecnologie di informazione e comunicazione*" [36]

estese a un insieme di oggetti che solitamente non vengono considerati come computer. L'Internet Of Things, infatti, descrive un insieme di oggetti (smart devices), dotati di sensori e di appositi software, che si connettono tra di loro e che generano, scambiano ed utilizzano i dati, spesso senza alcuna interazione umana. Non esiste virtualmente alcuna limitazione rispetto a quali oggetti possono diventare dei smart devices ed essere quindi connessi alla rete dell'Internet of Things, e questo rende l'ambito di applicazione di questa nuova tecnologia talmente esteso da poter essere considerato come una rivoluzione che andrà a impattare tutti gli ambiti della nostra vita.

L'utilizzo dell'IoT, infatti, spazia dall'utilizzo nella domotica, dando la possibilità di creare un'abitazione più efficiente sia dal punto di vista energetico che quello di gestione del tempo per le persone che ci vivono, fino all'utilizzo nelle Smart City, città 'intelligenti' che promettono di ridurre il problema del traffico e di sfruttare al meglio gli spazi pubblici, passando per l'ambito militare e industriale. Il numero sempre crescente di dispositivi connessi all'IoT (12.2 miliardi nel 2019) e il suo sempre più proficuo mercato (si contano 389 miliardi di dollari in questo settore) rendono questa tecnologia una delle più discusse del momento, sia per i vantaggi che potrebbe fornire sia per i danni che potrebbe causare [37].

### 2.1.2 Storia e funzionamento

#### Storia

Il termine Internet of Things fu utilizzato per la prima volta dall'ingegnere inglese Kevin Ashton nel 1999 per descrivere un sistema in cui gli oggetti del mondo fisico potessero essere connessi a internet. Anche se il termine è stato coniato recentemente, l'intuizione di collegare semplici oggetti (non computer) a Internet e farli comunicare tra loro è più antica e le sue origini possono venire fatte risalire agli anni '70: in questo periodo infatti erano già presenti dei sistemi per monitorare

da remoto i contatori elettrici [38]. Il passo successivo è stato quello di collegare effettivamente un oggetto a Internet: ciò è avvenuto quando un tostapane che poteva essere acceso e spento attraverso internet venne presentato a una conferenza nel 1990 [39]. Da allora vennero progettati ulteriori oggetti che potevano essere collegati alla rete, e venne a crearsi una disciplina di studio che si concentrava sullo studio e sullo sviluppo di 'reti di oggetti intelligenti' [40], il prototipo dell'attuale IoT.

Sebbene il concetto di IoT sia ormai vecchio più di 30 anni, è solo negli ultimi anni che si inizia a parlarne e a sviluppare un progetto più ampio e coeso. La motivazione principale è da ricercarsi nella confluenza di varie aree di studio e tecnologie:

- **Connettività ubiqua**: cioè la possibilità di avere una connessione attiva in qualsiasi momento e per qualsiasi cosa; ciò è stato possibile grazie a reti, soprattutto wireless, sempre meno costose e più veloci
- **Adozione su larga scala di reti basate sul protocollo internet**: nel tempo sempre più servizi hanno adottato il protocollo internet per permettere la comunicazione, rendendolo lo standard globale, facilmente implementabile in qualsiasi dispositivo e privo di costi particolari (ad esempio 15 anni fa il sistema di messaggistica non si basava quasi completamente sulla comunicazione internet come lo fa oggi)
- **Economie computazionali**: cioè il mercato relativo alla computazione (PC, smartphone...), in continuo e costante aumento; questo mercato è ovviamente indispensabile per la creazione di dispositivi IoT
- **Miniaturizzazione**: col tempo è stato possibile produrre microchip sempre di minori dimensioni, permettendo di incorporarli in oggetti molto piccoli; ciò ha reso possibile anche la costruzione di sensori di limitata grandezza permettendo a qualsiasi oggetto di diventare uno smart device

- **Analisi dei dati**: come vedremo, una delle principali attività da svolgere nel mondo IoT è l'analisi dei dati. Negli ultimi anni lo sviluppo in questo settore è stato enorme, permettendo la nascita di dataset estremamente grandi e metodi per analizzarli incredibilmente potenti
- **Cloud Computing**: cioè l'erogazione di servizi informatici offerti attraverso internet, che permettono di svolgere alcune operazioni, come il processamento dei dati, da remoto; questo ambito è fondamentale per permettere a dispositivi relativamente semplici di integrarsi e diventare funzionali nel mondo IoT

Negli ultimi anni ognuna di queste aree ha fatto importanti passi avanti e l'intersezione nei loro utilizzi ha permesso di rendere reale l'idea di una totale connessione tra dispositivi, con interferenze umane minime.

### Modelli di comunicazione

Come già affermato, la rivoluzione di questa tecnologia è data dalla comunicazione tra dispositivi diversi. Tuttavia non esiste un unico metodo di comunicazione, ma, anzi, la Internet Architecture Board (IAB) nel 2015 ne ha individuati ben quattro [41], ognuno dei quali offre possibilità differenti:

- **Dispositivo a Dispositivo**: questo è il caso in cui due dispositivi comunicano direttamente tra di loro, senza bisogno di alcun intermediario (a titolo d'esempio si possono considerare una lampadina e un interruttore che comunicano direttamente tra di loro). Questo tipo di comunicazione utilizza spesso tecnologie differenti dal protocollo internet, come ad esempio la tecnologia Bluetooth, ed è molto utilizzato nella Smart Home. Tuttavia, per far sì che ci sia una comunicazione diretta, i dispositivi devono utilizzare il medesimo protocollo e la medesima struttura dei dati inviati e ricevuti, rendendo difficile la compatibilità tra differenti gruppi di dispositivi. Sebbene questo crei senza dubbio una limitazione nella scelta dei possibili dispositivi da utilizzare, si ha

però la garanzia che questi comunichino molto bene ed efficientemente tra di loro

- **Dispositivo a Cloud**: in questo caso i dispositivi, anziché comunicare direttamente tra di loro, utilizzano come intermediario un servizio internet in cloud che si occupa di scambiare dati e messaggi tra i vari dispositivi connessi. Qui il protocollo maggiormente utilizzato è il protocollo internet, che sfrutta la vastissima rete già da tempo esistente, permettendo di utilizzare protocolli di comunicazione standard e assodati. Grazie a questo tipo di comunicazione è possibile estendere l'utilizzo originale dei dispositivi dotandoli di nuove funzionalità. Un esempio di questo tipo di comunicazione è l'utilizzo di un termostato 'intelligente': i dati raccolti dall'apparecchio vengono inviati in cloud e l'utente può controllarne l'utilizzo attraverso il suo smartphone. Rimane comunque la problematica dell'interoperabilità dei dispositivi: spesso, infatti, il servizio cloud e i dispositivi appartengono a uno stesso produttore che, se utilizza un protocollo di comunicazione personale, limita il possibile utilizzo di dispositivi di altri produttori
- **Dispositivo a Gateway**: questo modello è simile al precedente con la differenza che il dispositivo, prima di comunicare con il cloud, passa attraverso un Gateway, il cosiddetto Device-to-Application-Layer-Gateway(ALG), che fornisce varie funzionalità tra cui dei protocolli di sicurezza. Spesso i dispositivi utilizzati in questo caso non hanno la capacità di connettersi direttamente ai servizi cloud e devono necessariamente passare per un intermediario (gateway), che la maggior parte delle volte altro non è che lo smartphone dell'utente. Nonostante questo modello aumenti inevitabilmente la complessità del sistema, offre il vantaggio di poter integrare vari dispositivi che teoricamente sono incompatibili tra loro
- **Condivisione dei dati per Back-End**: utilizzando i modelli di comunicazione precedentemente descritti, è facile che i dati prodotti da dispositivi di

differenti produttori non siano accessibili e analizzabili insieme. L'architettura basata sulla condivisione dei dati per back-end risolve questa limitazione permettendo di esportare ed analizzare dati proveniente da sorgenti differenti. Per poter implementare questo modello è necessario un ecosistema in cui i differenti servizi cloud comunichino tra di loro attraverso un protocollo comune (usando delle API ad esempio). Per quanto promettente sia, questo modello necessita tuttavia un accordo comune tra diversi venditori di servizi IoT, il che può risultare spesso un problema insormontabile.

Considerando i quattro modelli appena presentati appare chiaro che un aspetto fondamentale nel mondo IoT sia l'utilizzo di standard non proprietari che permettano l'interoperabilità tra dispositivi; aspetto che, al giorno d'oggi, non è ancora stato del tutto approfondito e sviluppato [42].

### Architettura

Sebbene non sia possibile descrivere univocamente l'architettura dell'Internet of Things, ci sono quattro elementi indispensabili per un funzionamento completo e che sfrutti al massimo le sue potenzialità: la parte hardware degli oggetti (in particolare i microprocessori e i sensori e attuatori), la parte software degli oggetti (necessaria per il processamento dei dati e per il controllo delle funzionalità degli oggetti), il mezzo di comunicazione (comunemente si tratta di reti WiFi, Bluetooth e satelliti) e le piattaforme in cui conservare i dati (i servizi cloud).

Questi elementi sono gli attori principali nel ciclo di processamento dei dati e di controllo degli oggetti, che può essere visto come composto da alcuni layer, o stage, differenti, e riassunto nella *Figura* 2.1:

1. **Stage dei sensori e degli attuatori**: In questo stage i dati sono raccolti dai sensori presenti negli oggetti, e questi ultimi possono modificare il proprio stato attraverso gli attuatori. Per attuatore si intende un componente che può apportare delle modifiche all'oggetto a cui è collegato. Ad esempio, un

attuatore può cambiare lo stato di una lampadina spegnendola nel momento in cui i sensori rilevano una sufficiente luce solare all'interno della stanza. È possibile che in questo stage sia presente una più o meno elevata attività di processamento di dati in base al tipo e alla complessità dell'architettura analizzata

2. **Stage di acquisizione e trasferimento dei dati**: In questo stage i dati dai vari oggetti vengono raccolti e trasferiti verso il cloud. In base all'architettura utilizzata, è possibile che questo lavoro venga effettuato da un Gateway che, oltre a ricevere e inviare i dati, svolge anche delle funzioni relative alla sicurezza e al filtraggio dei dati. Può inoltre essere presente un dispositivo, chiamato Data Aquisition System(DAS), che svolge il lavoro di convertire i dati da analogici a digitali e di immagazzinarli prima di inviarli al Gateway

3. **Stage di edge**: Qui i dati vengono analizzati e pre-processati per ridurre il carico nella trasmissione dei dati, per poi essere inviati ai data center e alle piattaforme cloud

4. **Stage di analisi dei dati**: In questo stage i dati vengono analizzati nel dettaglio e conservati. Possono venire utilizzate varie tecnologie per processare in maniera automatica i dati: di particolare rilevanza sono senza dubbio le tecniche di Machine Learning, che, spesso, prendono in esame non solo i dati di un singolo utente ma di un numero elevatissimo di utenti, al fine di svolgere un'analisi statistica più estesa e individuare pattern altrimenti difficilmente identificabili

5. **Stage applicativo**: Sebbene il trasferimento e il processamento dei dati sia stato ultimato, e quindi in alcuni casi questa non venga definita una vera e propria fase nel ciclo IoT, rimangono da definire le azioni da compiere. Qui, ad esempio, l'utente può venire avvisato dell'attivazione di un allarme, anche se

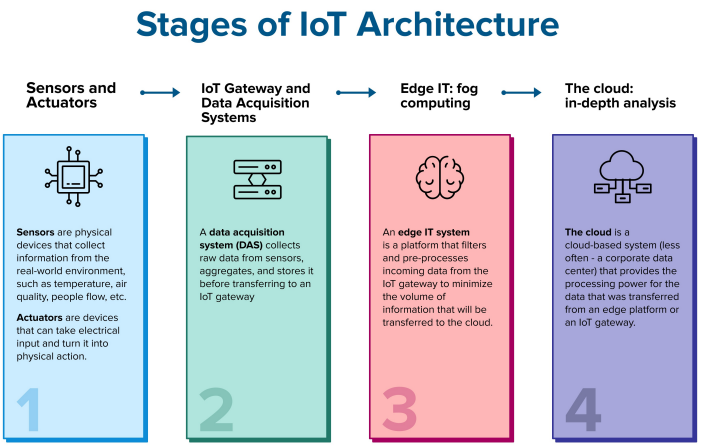



Figura 2.1: Gli stage di un sistema IoT(escluso quello applicativo)

spesso il sistema stesso prende decisioni in maniera autonoma su come comportarsi e su come modificare lo stato degli oggetti senza bisogno dell'intervento umano.

### 2.1.3 Utilizzi

Nonostante gli utilizzi dell'Internet of Things siano innumerevoli, si è soliti dividerli nelle sue quattro applicazioni principali: le applicazioni per il consumatore, le applicazioni organizzative, le applicazioni industriali e le applicazioni infrastrutturali.

- **Applicazioni per il consumatore**: con questo termine si intendono tutte quelle applicazioni acquistabili e utilizzabili dal singolo utente per il suo beneficio personale e non come mezzo per il guadagno economico o lo sviluppo tecnico e scientifico. Al momento, alcune delle tecnologie di questo tipo più diffuse sono senza dubbio i dispositivi indossabili: degli oggetti elettronici che interagiscono con lo smartphone dell'utente e che vengono indossati, solitamente al polso, tipicamente per raccogliere dati relativi all'attività fisica come battito cardiaco, pressione del sangue e calorie bruciate. Tra le altre applicazioni più diffuse si possono citare le Smart Home, che verranno discusse

approfonditamente più avanti, e le automobili connesse, delle auto che, comunicando con un servizio cloud, permettono di scegliere il percorso migliore, di trovare più facilmente parcheggio e di prevedere malfunzionamenti del veicolo prima che accadano

- **Applicazioni organizzative**: in questa categoria sono riunite quelle applicazioni che sono solitamente utilizzate in ambito pubblico e di larga scala. In questo ambito applicativo rientrano le applicazioni mediche, che possono essere sia utilizzate dal paziente nella sua vita quotidiana (ad esempio monitorando il pacemaker o controllando i vari valori vitali come pressione sanguigna e battito cardiaco) sia negli ospedali; molte strutture, infatti, stanno facendo uso tra le altre cose di letti dotati di sensori che possono accorgersi di quando un paziente sta cercando di alzarsi. Un altro importante ambito è sicuramente quello dei trasporti, in cui l'introduzione di tecnologie IoT potrebbe garantire un importante miglioramento nell'efficienza
- **Applicazioni industriali**: questa categoria è molto ampia, include infatti qualsiasi ambito industriale e spazia dall'industria manifatturiera fino a quella agricola. Qui, il continuo scambio e processamento di dati garantisce un controllo costante delle variabili in gioco, siano esse la temperatura e l'umidità del terreno o lo stato delle tubature per il trasporto di gas e petrolio, permettendo così di migliorare la produttività e l'efficienza delle aziende, portando a diminuire i costi e aumentare i guadagni
- **Applicazioni infrastrutturali**: uno degli obiettivi più ambiziosi del mondo IoT è quello di gestire l'intero ambiente cittadino in maniera automatizzata ed efficiente. Le Smart City, infatti, si prefiggono questo scopo: la costante e istantanea comunicazione tra le varie zone della città, unita all'incessante tracciamento e controllo di tutti i suoi elementi permettono una gestione totale e in sintonia dell'insieme, creando un ambiente in cui si massimizzi l'efficacia delle risorse e si minimizzino gli sprechi

## 2.2 Sicurezza nell'Internet Of Things

### 2.2.1 Rischi per la sicurezza

La criticità principale per lo sviluppo della tecnologia IoT, insieme forse al problema della frammentazione e a quello della privacy che verrà analizzato nella prossima sezione, è senza dubbio la questione della sicurezza. Sebbene la maggior parte degli aspetti legati alla sicurezza nel mondo IoT non sia diversa da quella tipica di un sistema informatico generico, ciò che cambia in questo caso è la scala e il raggio d'azione dei possibili danni. L'architettura stessa del mondo IoT, infatti, con ogni oggetto che diventa un potenziale punto d'ingresso nel sistema, risulta per sua stessa natura più vulnerabile ad attacchi informatici che, con l'interconnessione dei dispositivi su larghissima scala, hanno la possibilità di intaccare facilmente più aree di interesse.

Il maggior rischio della tecnologia IoT risiede nel fatto che una volta che un attaccante prende controllo di un dispositivo, l'attacco può facilmente propagarsi ai dispositivi connessi, e, vista l'elevata connettività di questi ambienti, non risulta difficile prendere il controllo dell'intero sistema. Inoltre, un altro importante aspetto da considerare è il fatto che oggetti che in principio erano isolati ora sono connessi a internet e quindi vulnerabili; a titolo d'esempio, risulta possibile connettersi a un'automobile smart e controllare da remoto il funzionamento dei freni, azione che sarebbe impossibile per una vettura classica.

Le conseguenze di attacchi agli smart device possono essere, già al giorno d'oggi, molto gravi, ma lo saranno ancora di più in futuro visto il trend di utilizzo di questi dispositivi: la nostra abilità di svolgere le attività quotidiane senza connessione internet decrescerà col tempo, obbligandoci ad utilizzare in misura sempre maggiore dispositivi IoT e diventandone sempre più dipendenti, aumentando la gravità dei danni di un attacco (è indicativo di questo trend il fatto che diventa sempre più complicato acquistare dispositivi che non si possano connettere a internet).

Se, ad esempio, risulta innocuo lo spegnimento di una smart TV per interrompere un attacco, non è così semplice scollegare un sistema di semafori di una città o il pacemaker di una persona [43].

### Esempi di attacchi

Può senza dubbio risultare utile citare qualche esempio di attacco in ambito IoT per avere un'idea più specifica delle debolezze, delle conseguenze e del raggio d'azione in quest'area d'interesse.
L'attacco più celebre è probabilmente il Distributed Denial of Service, DDoS[2], del 2016 causato dal malware Mirai. Mirai è stato progettato per infettare dispositivi connessi a internet, e specialmente dispositivi IoT, rendendoli parte di una rete usata per effettuare attacchi DDoS. Il malware è riuscito ad infettare milioni di dispositivi di svariato genere (telecamere di sorveglianza, home gateway, baby monitor...), tutti quasi privi di protezione, e in particolare si è diffuso facilmente nelle reti domestiche. Nel 2016, i dispositivi infettati hanno attaccato il servizio di DNS Dyn, impedendo a una grossa percentuale di utenti in Nord America ed Europa di visitare alcuni siti tra cui Amazon, Spotify e Paypal [44]. Questo attacco, che ha colpito prodotti di grosse aziende quali Dahua, Huawei e Cisco, è stato causato da una scarsa implementazione del processo di comunicazione tra le varie componenti software del sistema, causando una forte preoccupazione tra gli esperti di sicurezza informatica [45].
Un altro attacco che vale la pena citare è quello avvenuto nel Marzo del 2021 quando un gruppo di hackers è riuscito ad accedere e a controllare migliaia di telecamere che utilizzavano il servizio di Verkada, un'azienda della Silicon Valley che vende una

[2]Il Denial of Service è una tipologia di attacco informatico che consiste nell'esaurire deliberatamente le risorse del sistema attaccato in modo che non possa più fornire servizi. Il Distributed Denial of Service è una sottocategoria di questo attacco in cui l'obiettivo è attaccato da più fonti contemporaneamente

tipologia di servizi noti come SECurity as a Service,SECaaS [3]. L'attacco è riuscito grazie alla scoperta di credenziali di utenti pubblicamente rintracciabili su Internet. Da qui sono riusciti a muoversi nella rete fino a prendere controllo di un account di un amministratore, avendo così il controllo sulle telecamere. Una delle cose preoccupanti è il fatto che l'azienda ha scoperto dell'attacco solamente una volta che gli attaccanti hanno reso note le loro azioni [46].
Infine, viene riportato un attacco che fa capire le conseguenze della connessione di dispositivi un tempo isolati e dei possibili danni sul singolo individuo. Nel 2015 un team di ricercatori è riuscito, attraverso il canale che permette la comunicazione dei vari componenti del veicolo, di prendere il totale controllo di una Jeep, facendola accelerare, decelerare e muovere il volante [47]. In questo caso, le conseguenze potrebbero essere fatali per l'utilizzatore del dispositivo IoT.

### Sfide nel mondo della sicurezza IoT

L'utilizzo di dispositivi IoT che abbiano un'elevata garanzia di sicurezza è ovviamente un'azione fondamentale per mitigare i possibili rischi di un attacco informatico; tuttavia, è impossibile creare un prodotto completamente sicuro, ed è importante ricordare che, usando le parole di Bruce Schneier[4], *la sicurezza è un processo e non un prodotto.* Ciò che si vuole dire con questa frase è che, con gli sviluppi tecnologici e con le continue scoperte, ciò che un tempo era sicuro può non esserlo più; le misure di protezione utilizzate vengono superate da nuove tipologie di attacchi che portano a un aggiornamento delle stesse misure, risultando in un circolo virtualmente infinito, che non lascia spazio a un concetto di sicurezza informatica fisso e stabile nel tempo.

[3]queste aziende vendono tramite abbonamenti mensili dei servizi di sicurezza che vengono implementati in prodotti di aziende terze

[4]Bruce Schneier è un crittografo e saggista statunitense, scrittore di numerosi volumi, in particolare Crittografia pratica (Applied Cryptography), che è diventato un libro di riferimento per la crittografia

Oltre a questa criticità, è possibile elencare altri fattori che influiscono nello sviluppo di tecnologie con un elevato livello di sicurezza tra cui:

- **Costo**: Naturalmente, il costo economico per implementare le adeguate misure di sicurezza è un fattore fondamentale. Solitamente, si sviluppa un diverso livello di sicurezza, avendo così un costo differente, in base al danno che può causare un potenziale attacco. Così, si andrà a implementare maggiormente la sicurezza, spendendo più soldi, in casi come un sistema medico, mentre per dispositivi come frigoriferi si investirà meno, rendendoli però più vulnerabili. Ovviamente, il costo economico non si calcola soltanto durante lo sviluppo del dispositivo, ma si devono considerare i danni economici e d'immagine che un attacco potrebbe causare. In questo caso, un'azienda può essere spinta ad investire maggiormente in sicurezza temendo le possibili multe che potrebbe ricevere e la pubblicità negativa che potrebbe causare un attacco ai suoi prodotti

- **Limitazione computazionale**: Molti smart devices hanno una capacità computazionale molto limitata. Questo rende difficile implementare forti sistemi di sicurezza al loro interno, come ad esempio un sistema di cifratura complesso o l'utilizzo di un firewall [48]

- **Larga scala**: Molti smart devices sono pensati per essere prodotti su larghissima scala, a livelli molto più grandi dei dispositivi classici. Come risultato, la connessione tra questi dispositivi diventa enorme; inoltre comunicando tra di loro senza intervento umano, risulterà complicato predire il comportamento e rilevare anomalie

- **Omogeneità**: Un sistema IoT conterrà al suo interno un elevato numero di dispositivi identici a loro (ad esempio, delle lampadine in un edificio). Ciò significa che una vulnerabilità di un elemento sarà ingigantita a causa dell'elevata presenza di questo all'interno del sistema

- **Visibilità**: Oltre al fatto che spesso i dispositivi lavorano in una maniera in cui l'utente non abbia visibilità dell'attività interna o del flusso di dati che inviano, molti di questi sono posizionati in punti poco visibili, rendendo il monitoraggio e la rivelazione di problemi particolarmente complicato
- **Aggiornamento**: Una delle attività fondamentali per garantire un corretto livello di sicurezza dei dispositivi informatici è il loro costante e periodico aggiornamento. Tuttavia, molti dispositivi IoT sono sviluppati in modo che sia impossibile o molto difficile effettuare un aggiornamento. Emblematico è il caso del 2015 in cui la Fiat Chrysler ha dovuto richiamare 1.4 milioni di veicoli a causa di una vulnerabilità che ne permetteva l'hackeraggio. In questo caso, i proprietari delle automobili interessate avrebbero dovuto portarle in un centro dell'azienda o effettuare tramite chiavetta USB l'aggiornamento loro stessi. Vista la difficoltà e la scarsa consapevolezza media dei pericoli informatici, una grande percentuale di veicoli non è stata aggiornata, lasciando inalterata la vulnerabilità [43]

### 2.2.2 Rischi per la privacy

Il rischio per la privacy nei sistemi IoT è chiaro: l'intero suo funzionamento si basa sull'acquisizione e sul processamento dei dati, spesso dati personali dell'utente. Nello stadio di analisi dei dati analizzato nella sezione precedente, si nota come i dati non rimangano in mano all'utente ma vengano inviati a servizi cloud in cui vengono analizzati e conservati, introducendo possibili violazioni della privacy dell'utente.

I rischi di questa nuova tecnologia sono così grandi che qualcuno è arrivato a considerarla un potenziale strumento per il controllo sociale e la manipolazione politica [49]. Senza dubbio, il suo utilizzo, se privo di norme adeguate, può essere una minaccia per l'individuo sia se effettuato da aziende private sia se effettuato da enti pubblici e governi. Sebbene la diffusione in quest'ultimo ambito sia al momento

minore rispetto a quello privato, le sempre più presenti opere di larga scala, come ad esempio le Smart City, fanno presagire un suo inevitabile inserimento negli spazi pubblici.

Inoltre, come visto nella sezione precedente, l'architettura IoT risulta particolarmente esposta ad attacchi hacker, che potrebbero causare il furto di dati personali. L'esempio riportato precedentemente, del controllo di telecamere di sicurezza da parte di individui non autorizzati, esemplifica perfettamente il rischio di intrusione illecita nelle vite private delle persone.

Tra i personaggi più critici rispetto a questa tecnologia, si può citare Peter-Paul Verbeek, un professore di filosofia della tecnologia olandese, che ribadisce come la tecnologia non debba essere vista come uno mero strumento inerte, ma come un agente attivo, che influenza le nostre scelte morali e cambia la nostra concezione di privacy e autonomia [50]. Lo scrittore Adam Greenfield afferma che la tecnologia IoT non solo è un'invasione dello spazio pubblico, ma è anche utilizzata come strumento per normare il comportamento degli individui, citando un cartellone pubblicitario con telecamere nascoste che tracciava i passanti che si fermavano a leggerlo, ignari di ciò. Infine, la American Civil Liberties Union, un'organizzazione non governativa orientata a difendere i diritti civili e le libertà individuali negli Stati Uniti, parla di questa tecnologia così: "*Semplicemente non c'è modo per predire come questi immensi poteri - sproporzionalmente accumulati nelle mani di corporazioni che puntano al vantaggio economico e di governi che bramano ancora più controllo - verranno utilizzati. Le probabilità sono che i Big Data e l'Internet of Things complicheranno la nostra capacità di controllare le nostre vite, col fatto che diventiamo sempre più visibili e trasparenti alle aziende e istituzioni mentre loro diventano per noi sempre più imperscrutabili e opachi* [51]".

### Aspetti unici in ambito IoT

L'Internet of Things, sebbene per certi aspetti sia molto simile agli altri sistemi informatici, presenta degli aspetti unici che sono intrinsecamente collegati alle questioni della privacy come:

- **Interazione con l'utente**: Uno dei metodi tradizionali a disposizione dell'utente per salvaguardare la sua privacy è gestire delle impostazioni e preferenze relative ad esse (ad esempio i checkbox 'I agree') interfacciandosi con lo schermo del dispositivo. Tuttavia, un aspetto fondamentale dei dispositivi IoT è la loro capacità di funzionare senza intervento umano, e alcuni di essi non possiedono alcun meccanismo con cui l'utente possa interfacciarsi. Risulta chiaro quindi che selezionare delle impostazioni relative alla privacy in questi dispositivi risulta impossibile se non attraverso mezzi esterni
- **Larga scala**: Come ribadito più volte, un sistema IoT, ad esempio una Smart Home, è composto da un numero elevatissimo di dispositivi. Controllare le impostazioni di privacy dell'intero sistema risulta quindi complicato, considerando che i dispositivi potrebbero analizzare diverse categorie di dati e che potrebbero appartenere a diversi produttori. In questo caso, un'impostazione univoca per tutti i dispositivi sarebbe impossibile, ma anche gestirli singolarmente uno ad uno sarebbe impraticabile per l'utente
- **Spazi privati e pubblici**: Uno dei cambiamenti più importanti che l'IoT sta causando è quello di portare negli spazi privati dei dispositivi e delle tecniche che erano principalmente concepiti per gli spazi pubblici, andando ad assottigliare il diverso senso di privacy che si ha per questi due spazi distinti. Un esempio lampante di questa situazione è l'utilizzo di telecamere di sorveglianza connesse a internet: normalmente accettate negli spazi pubblici dove il livello di privacy è relativamente basso, stanno venendo pian piano utilizzate in casa, senza la completa consapevolezza che le immagini che acquisiscono spesso

vengono inviate a terzi

- **Influenza su altre persone**: Un importante fattore da considerare è come questi dispositivi abbiano un'influenza anche sulle persone che non li possiedono. I dispositivi IoT, infatti, spesso agiscono in ambienti con altre persone oltre al suo proprietario, raccogliendo dati relativi a chiunque si trovi nelle vicinanze. Ad esempio, un geolocalizzatore posto in un'automobile traccerebbe non soltanto il proprietario, che probabilmente avrà dato il consenso, ma anche possibili ignari passeggeri, senza che abbiano espresso nessuna preferenza a riguardo.
- **Big Data**: Un aspetto critico per la privacy in generale è l'aggregazione di dati personali differenti per una profilazione più dettagliata, precisa e ad ampio raggio. Nel mondo IoT questo problema è massimizzato. Vista la varietà di utilizzi dei dispositivi IoT, e soprattutto considerando che hanno accesso agli aspetti più intimi e privati di una persona, i dati raccolti possono fornire informazioni su un individuo a un livello di dettaglio senza precedenti, creando un concreto pericolo di danno e discriminazione.
- **Visibilità**: Molti dei dispositivi IoT sono pensati per essere invisibili o poco percepibili dalle persone. Si crea quindi il problema di non avere piena consapevolezza di quando e dove vengono raccolti i dati, creando un senso di incertezza rispetto alla presenza o meno di questi dispositivi. Questo ovviamente incrementa le difficoltà degli individui di salvaguardare la loro privacy.
- **Falso senso di sicurezza**: La presenza massiva di dispositivi IoT, nonché il loro utilizzo in ambienti sempre più ampi, può portare a un falso senso di sicurezza, portando gli utenti a divulgare informazioni private senza la giusta consapevolezza delle conseguenze.

# Capitolo 3

# SIFIS-HOME

## 3.1 Smart Home

Il lavoro fatto per questa tesi è parte del più ampio progetto di SIFIS-HOME, il cui centro d'interesse è la Smart Home; in questa sezione verrà dunque approfondito quest'ambito, andando ad analizzare le sue unicità rispetto alle altre applicazioni IoT descritte nel precedente capitolo.

### 3.1.1 Considerazioni generali

Il termine Smart Home si riferisce ad un'abitazione che offre la possibilità di gestire, in maniera automatica o da remoto, i suoi impianti e dispositivi al fine di risparmiare energia, semplificare la vita domestica e garantire la sicurezza delle persone che la abitano. All'interno della Smart Home è possibile integrare vari dispositivi IoT, di produttori differenti, rendendo questo ambiente particolarmente incline alle problematiche del mondo IoT descritte nel capitolo precedente, aggravate dal fatto che molto spesso il proprietario della Smart Home non è un esperto in queste tematiche e non è a conoscenza dei rischi del suo utilizzo.

**Storia**

La Smart Home è l'ultimo prodotto di una più ampia area di ricerca che prende il nome di domotica (dall'unione del termine domus, che in latino significa "casa", e del suffisso greco *ticos*, che indica le discipline di applicazione), una scienza interdisciplinare, nata dall'unione di vari ambiti quali l'edilizia, l'informatica, l'elettronica e le telecomunicazioni, che si occupa dello studio delle tecnologie atte a migliorare la qualità della vita nella casa.

La storia della domotica, in un senso generale, si può fare iniziare già dalla fine dell'Ottocento/inizio Novecento con l'introduzione dei primi elettrodomestici: in questo periodo infatti vengono introdotti lo scaldabagno (1889), la lavatrice (1904), il frigorifero (1913) e la lavastoviglie (1929). Un curioso primo esempio di una primordiale Smart Home si ha nel 1966 quando l'ingegnere Jim Sutherland presenta ECHO IV, un computer con vari display e tastiere sparsi per la casa che permettevano il controllo di varie funzionalità, tra cui l'accesso alla televisione, l'uso dell'aria condizionata e il controllo di tutti gli orologi digitali in essa. I veri sviluppi di una più moderna domotica, tuttavia, avvengono nel 1975, anno in cui viene presentato l'X10, uno standard per la comunicazione tra dispositivi elettronici che utilizza l'impianto elettrico della casa per inviare messaggi tra i vari dispositivi; sebbene ormai abbia più di 40 anni rimane ancora uno degli standard più utilizzati nel mondo della domotica. Negli anni '80 gli sviluppi si fecero sempre più frequenti con l'introduzione di porte automatiche, termostati programmabili e sistemi di sicurezza economici e diffusi, fino ad arrivare al primo tostapane collegato ad internet nel 1990, che segnò l'inizio dell'era dell'Internet of Things. Da allora gli smart devices hanno dominato il settore, e con l'introduzione di assistenti vocali accessibili ed economici come Alexa la loro diffusione nella vita quotidiana delle persone comuni è un dato di fatto.

### Influenza

Quello della Smart Home è un mercato, come tutte le tecnologie IoT, in espansione, e a inizio 2022 si stimavano 258 milioni di Smart Home presenti in tutto il mondo, con gli Stati Uniti che sono la nazione che ne possiede di più seguita dalla Cina. Secondo alcune prospettive future, entro il 2026 il numero di Smart Home crescerà raggiungendo il numero di 573 milioni.
Per quanto riguarda il guadagno economico, questo mercato genera un ricavo di 103 miliardi di euro a livello globale, con gli Stati Uniti che hanno un mercato di 28 miliardi di euro, la Cina di 21 miliardi e l'Europa (Russia esclusa) di 25 miliardi. Anche in questo caso le prospettive future sono rosee, con una predizione di 167 miliardi di euro a livello mondiale entro il 2026. [52]

### Ambiti di applicazione

Le macroaree di possibile automazione della casa sono principalmente quattro:

- **Gestione dell'ambiente**: la presenza di un sistema di sensori e attuatori permette la termoregolazione di ogni singola stanza dell'abitazione, cambiando la temperatura in base a vari fattori, siano relativi a un risparmio energetico, alla presenza di persone all'interno o semplicemente per comfort. Questi sistemi permettono anche una gestione dell'illuminazione domestica con i medesimi obiettivi, così come di un possibile sistema d'irrigazione
- **Gestione degli apparecchi**: in questo ambito si punta a un maggiore gestione e coesione degli elettrodomestici, migliorando le prestazioni, le funzionalità e l'affidabilità di lavatrici, lavastoviglie, asciugatrici e forni
- **Comunicazione e informazione**: qui rientra la gestione delle comunicazioni da e verso la casa, sia attraverso telefoni che attraverso citofoni. Questo ambito

permette agli utenti di interagire, possibilmente in maniera semplice, efficiente e sicura, con l'abitazione anche da remoto

- **Sicurezza**: con questo termine non s'intende una sicurezza informatica atta a proteggere il sistema IoT contro attacchi hacker, bensì un miglioramento delle classiche funzioni di difesa dell'abitazione. In questo ambito si può citare l'uso di telecamere e allarmi che avvertono in automatico le autorità competenti. Altra applicazione importante per la sicurezza è il meccanismo di controllo di fughe di gas, incendi, allagamenti e altri eventi dannosi.

All'interno di queste tre macroaree, si possono individuare 11 categorie d'applicazione a cui un device può fare riferimento: illuminazione, energia e gas, intrattenimento, benessere e salute, sicurezza, monitor per bambini e animali, vestiti e accessori, veicoli e droni, robot domestici, giardinaggio, soluzioni integrate.

### Livelli d'integrazione della Smart Home

Ovviamente, un'abitazione non può essere classificata in maniera binaria come 'tradizionale' o 'smart', ma è importante definire vari livelli che vanno da una casa in cui non è presente alcun dispositivo IoT a una casa pensata e progettata per essere completamente integrata nel mondo IoT, passando per quelle abitazioni che possiedono solo qualcuno di questi device, come quelle in cui è presente solamente un dispositivo di riconoscimento vocale come Alexa. È possibile distinguere 6 livelli di integrazione dalla Smart Home, riassunti nella *Figura* 3.1 e ora brevemente descritti:

- **Livello 0**: Una casa priva di qualsiasi tecnologia IoT.
- **Livello 1**: Una casa con qualche device, come una televisione smart o un baby monitor. In questo livello il proprietario ha il pieno controllo della casa interagendo con essa in maniera analogica

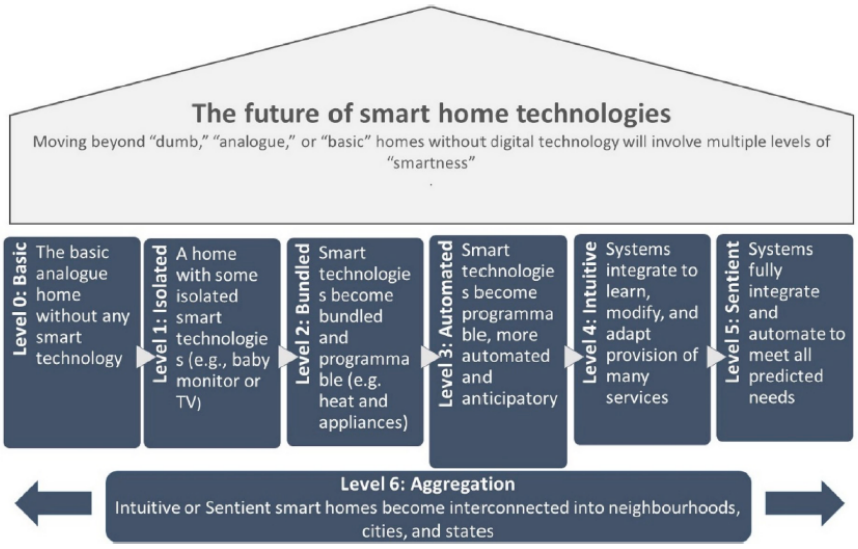



Figura 3.1: I 6 livelli di 'intelligenza' di una casa

- **Livello 2**: A questo livello la casa possiede tecnologie interconnesse e integrate per offrire sevizi più complessi come una gestione del riscaldamento e dell'intrattenimento

- **Livello 3**: Qui iniziano a vedersi dei segni più importanti di automazione, con il sistema più interconnesso e in grado di anticipare alcune azioni, come ad esempio accendendo le luci quando una persona entra nell'abitazione

- **Livello 4**: A questo livello l'abitazione inizia a imparare e ad adattarsi, anche in base a un contesto più ampio (ad esempio poterebbe controllare l'illuminazione in base alle condizioni atmosferiche). Grazie a un sistema di feedback fornito da sensori e monitor la casa può modificarsi per accontentare al meglio gli utenti

- **Livello 5**: A questo livello la casa è completamente smart, anticipando tutte le necessità dell'abitazione. Tutte le sue parti sono interconnesse e comunicanti tra loro, e riuscirebbe a comunicare direttamente all'utente

### 3.1.2 Pro e Contro

Nel 2019 Benjamin K. Sovacool e Dylan D. Furszyfer Del Rio presentarono uno studio [53] in cui descrivevano l'attuale panorama dell'ambiente della Smart Home, analizzandone benefici, rischi e barriere all'implementazione di questi sistemi. I due ricercatori hanno condotto svariate interviste, principalmente nel Regno Unito, in ambiti diversi includendo figure governative, accademici, settori privati come Microsoft e Amazon, istituti di ricerca indipendenti, gruppi industriali e associazioni intergovernative. Sono inoltre state fatte visite alle aziende e ai negozi di dispositivi associati alla Smart Home, e i dati sono stati confrontati e ampliati con altri studi precedenti. In seguito, sono riassunti i risultati ottenuti.

#### Benefici

Tra i benefici principali che sono stati individuati nelle varie interviste riguardo l'uso di Smart Home ci sono:

- **Gestione dell'energia**: Questo sembra essere il beneficio maggiore dato da un'abitazione connessa al mondo IoT. Il continuo monitoraggio e controllo da parte dei sensori e attuatori permette una gestione più efficiente dell'energia della casa. Questo beneficio è particolarmente rilevante probabilmente a causa della grande inefficienza dei tradizionali sistemi di riscaldamento: secondo alcuni studi condotti nel Regno Unito, il 95% delle case possiede un riscaldamento centralizzato la cui massima possibilità di gestione è un interruttore per spegnere o accendere il riscaldamento; inoltre, si stima che 800mila abitazioni non hanno controllo dello scaldabagno e che 8 milioni di abitazioni non hanno un termostato per ogni stanza

- **Convenienza e controllo**: A pari livello d'importanza si colloca la questione del comfort e del controllo. In questo ambito hanno molto risalto le tecnologie

di controllo vocale come Alexa che permettono un minore impegno in alcune attività domestiche

- **Benefici economici**: Viene vista molto positivamente l'abilità della Smart Home di monitorare meglio le spese domestiche e di permettere di passare a tariffe più convenienti e fornitori di servizi più economici

- **Benefici per gli operatori**: Non è solamente l'utente a poter beneficiare dei vantaggi di una Smart Home ma anche le aziende e l'industria grazie all'ampissima quantità di dati che ricevono e per la possibilità di gestire da remoto e automaticamente alcuni aspetti che tradizionalmente richiedono l'intervento umano sul posto

- **Benefici ambientali**: Viene fatta molta leva su quest'aspetto, come si può vedere dalla *Figura* 3.2. I vantaggi in questo caso rimandano alla possibilità della casa di gestire al meglio le fonti energetiche e monitorare la quantità di C02 prodotta. Un'interconnessione di Smart Home, inoltre, faciliterebbe e migliorerebbe la distribuzione energetica all'interno di una città

- **Estetica**: Tra i benefici non si può non considerare il valore simbolico che questi device possono avere come elementi di stile e di moda. Al giorno d'oggi, possedere smart device in casa può indubbiamente essere visto come un simbolo di status

- **Salute**: La capacità della casa di allertare le autorità in caso di malessere e di monitorare la salute delle persone, soprattutto degli anziani e dei più deboli, è uno dei principali vantaggi di questa tecnologia e uno dei più apprezzati

- **Benefici sociali**: In questo ambito sono inclusi sia i benefici legati a una maggiore connessione, legati ad esempio all'ambito lavorativo dei residenti, sia i benefici legati alla possibilità di maggiore socializzazione e aiuto a stati emotivi come depressione e isolamento


Figura 3.2: Pubblicità di Smart Energy GB per la promozione di contatori intelligenti, Novembre 2018.

- **Educativi**: Questa tecnologia permette di rivoluzionare il mondo dell'educazione, rendendolo più interattivo, coinvolgente e connesso. Un esempio sono i robot sviluppati da Apple, che aiutano sia l'apprendimento generale dei bambini che quello specifico di alcune attività degli adulti
- **Intrattenimento**: Quest'ambito include aspetti come migliori e più facili modi di ascoltare musica o di guardare film e video in generale
- **Sicurezza**: La Smart Home offre la possibilità di monitorare e prevenire fughe di gas o incendi, nonché di avvisare le autorità competenti

### Rischi e barriere

In questa sezione vengono riportati sia i rischi relativi alla Smart Home sia le attuali barriere che ne impediscono un utilizzo più ampio.

- **Privacy e sicurezza informatica**: Come facilmente immaginabile, le preoccupazioni principali nell'adozione di questa tecnologia, come tutte le tecnologie IoT, riguardano la privacy e la sicurezza informatica, aumentate ancora di più dal fatto che questa tecnologia va a toccare la parte più intima e privata della nostra vita quotidiana

- **Affidabilità tecnologica e obsolescenza**: Un'altra percezione negativa relativa a questa tecnologia riguarda la convinzione, non del tutto sbagliata, che la complessità e le varie dipendenze vadano ad erodere l'affidabilità dei prodotti. Inoltre, un'altra preoccupazione riguarda la gestione della casa in caso di incidenti: in caso di blackout, per esempio, la maggior parte dei dispositivi, essenziali per un corretto funzionamento delle attività domestiche, potrebbero non funzionare. Infine, si considera l'incredibile velocità di sviluppo del settore che rischia di rendere velocemente datati i nuovi dispositivi

- **Usabilità e apprendimento**: Una barriera importante riguarda l'usabilità di questi dispositivi e la difficoltà ad imparare ad utilizzarli correttamente. Questa difficoltà non riguarda solamente il tempo necessario ad imparare e abituarsi all'utilizzo di un nuovo dispositivo integrandolo nelle abitudini quotidiane, ma riguarda molto spesso l'innata complessità di questi dispositivi e le loro innumerevoli impostazioni. Emblematico è il caso riportato nello studio, in cui si cita una persona che ha impiegato 11 ore per capire come far bollire l'acqua con un bollitore 'intelligente', esemplificando la diffusa concezione che queste tecnologie spesso complicano la vita invece di semplificarla

- **Elitarismo, barriere del mercato ed erosione della democrazia**: Questa problematica riguarda l'idea che le grandi aziende e i governi utilizzino i dati forniti da questa tecnologia più per i loro guadagni e fini che per un positivo impatto sociale. Si può certamente discutere del fatto che il sempre crescente potere che hanno queste aziende, insieme alle loro politiche spesso

opache, inclini al lobbismo e sfavorevoli alla tassazione, minaccino il sistema democratico e aumentino la disuguaglianza tra la popolazione

- **Interoperabilità**: l'interoperabilità è uno delle problematiche maggiori nel mondo dell'IoT, e riguarda il fatto che device prodotti da diverse aziende hanno difficoltà a comunicare correttamente tra loro
- **Consumo di energia**: Questo aspetto è contrapposto al beneficio precedentemente riportato riguardo il risparmio energetico. In verità solo una parte di questi device ha tra gli obiettivi principali quello della riduzione del consumo dell'energia, la maggior parte dei dispositivi punta invece all'aumento di comfort, causando anzi un maggior consumo di energia
- **Risorse e sostenibilità**: Strettamente collegato al punto precedente, questa tematica riguarda l'impatto ambientale che hanno questi dispositivi, soprattutto riguardo l'estrazione dei materiali necessari alla produzione. Spesso l'estrazione comporta infatti un danno sia ecologico che sociale, vista la localizzazione di questi materiali nelle aree più povere del pianeta
- **Perdita di controllo e autonomia personale**: Lasciare sempre più controllo delle attività quotidiane a un sistema computerizzato potrebbe portare ad un senso di perdita di controllo ed autonomia
- **Mancanza di proprietà della casa**: La percentuale di persone che hanno effettivamente possesso di un'abitazione e non sono solamente in affitto è incredibilmente bassa, e questo trend non sembra cambiare nel futuro prossimo. Questa è sicuramente una barriera per l'introduzione di queste tecnologie.
- **Mancanza di connessione internet**: Ovviamente la mancata o scarsa connessione internet, soprattutto nelle aree rurali e più povere è un ostacolo importante per la diffusione della tecnologia
- **Fiducia nelle aziende**: Una mancata fiducia nelle aziende, sia per quanto riguarda l'utilizzo dei dati che per quanto riguarda la loro disponibilità alla

risoluzione dei problemi è un ostacolo importante da considerare

- **Costo**: I dispositivi smart sono tipicamente più costosi delle loro controparti più tradizionali, disincentivando il loro acquisto
- **Isolamento sociale e solitudine**: Questo aspetto è contrapposto a un precedente beneficio citato precedentemente, ed in effetti sono facce opposte della stessa medaglia. Se da un lato questa tecnologia può facilitare la cura di persone fragili e anziani, dall'altro porta a rimpiazzare le interazioni personali causando un sentimento di solitudine e isolamento

### 3.1.3 Critiche

#### Capitalismo della sorveglianza

Tra i principali scettici dell'utilizzo della Smart Home, e della tecnologia IoT in generale, è impossibile non citare Shoshana Zuboff, autrice e psicologa sociale statunitense, che si occupa di tematiche riguardanti la rivoluzione digitale, l'evoluzione del capitalismo e le condizioni per lo sviluppo umano. Nel suo libro 'Il Capitalismo della Sorveglianza' [54], Zuboff descrive un progetto chiamato "Aware Home", una specie di modello di Smart Home sviluppato nel 2000 da un gruppo di ingegneri e informatici della Georgia Institute of Technology. Secondo la Zuboff questo modello differiva dagli attuali modelli di Smart Home per un principio fondamentale: la proprietà dei dati.

L'idea base nell'implementazione dell'"Aware Home", infatti, è che gli strumenti e le conoscenze della casa debbano appartenere al proprietario dell'abitazione e solo lui debba avere il diritto di utilizzarli. Questo è in netto contrasto con le attuali politiche aziendali del mercato della Smart Home che, sempre secondo l'autrice, sono fondate e hanno alla loro base la compravendita dei dati personali degli utenti e l'invasione della loro privacy. Come esempio vengono citati i termostati Nest, dispositivi IoT di proprietà Alphabet, l'azienda madre di Google, che inviano ai

loro server i dati dell'utente. Per Zuboff, quest'acquisizione, unita all'imponente sistema di raccolta dati che dispone Google, crea una disparità di conoscenza e potere enorme tra l'azienda e l'utente, rendendo quest'ultimo una fonte di guadagno da cui estrarre conoscenza piuttosto che l'effettivo beneficiario del servizio. Questo, rimarca l'autrice, è in netto contrasto con l'idea che guidava gli sviluppatori di "Aware Home" che sostenevano che visto il "*costante monitoraggio di ogni attività dei residenti, comprese le condizioni mediche, c'è una chiara necessità di fornire agli utenti la conoscenza e il controllo della distribuzione di queste informazioni per garantire la privacy delle informazioni degli individui*".

### Dualismo del controllo

Molte controversie riguardano il tema del controllo, ed è chiaro che ci sono due posizioni ideologicamente contrastanti: da un lato c'è chi elogia la Smart Home perché pone al centro l'individuo e ne aumenta il controllo, dall'altro lato c'è chi critica questa tecnologia perché, al contrario, toglie il controllo dalle mani dell'individuo. Questa dualità può venire riassunta dalla questione della gestione energetica. La Smart Home, infatti, permette all'utente di compiere scelte più informate considerando l'impatto che esse hanno come costo energetico; tuttavia, allo stesso tempo, esiste l'idea che le scelte migliori riguardo l'impatto energetico avvengano quando l'abitazione sceglie in maniera autonoma escludendo l'utente.
Un altro modo di vedere la questione del controllo è distinguerlo in 3 tipi: il controllo tecnologico, cioè l'abilità fisica di usare la tecnologia; il controllo percettivo, che è legato ai tentativi di controllare i pattern di consumo, di comportamento e anche emotivi; infine, il controllo relazionale, che si estende in senso più ampio alla gestione della vita quotidiana di una persona e delle sue relazioni interpersonali. Considerando questi tipi di controllo, l'influenza della Smart Home è ambigua, creando la potenzialità di andare ad incrementare il controllo tecnologico diminuendo invece il senso di controllo percettivo e relazionale.

## 3.2 SIFIS-HOME

Il progetto SIFIS-Home, o Secure Interoperable Full-Stack Internet of Things for Smart Home, è un progetto finanziato dall'Unione Europea attraverso il programma Horizon 2020 che ha come scopo la progettazione di un framework secure-by-design (sicuro sin dalla progettazione) e coerente, che migliori la sicurezza e la resilienza di sistemi interconnessi di case intelligenti (Smart Home) a tutti i livelli di stack. Per poter raggiungere l'obiettivo, il framework abilita (rivolgendosi agli sviluppatori di software e consentendogli di caricare i loro prodotti nella piattaforma), lo sviluppo di applicazioni, algoritmi e servizi che mettano al centro la sicurezza e la privacy, rendendo possibile la rilevazione e reazione ad attacchi informatici, tentativi di intrusione e violazione delle policy concordate con l'utente. Il framework così sviluppato andrà ad aumentare e consolidare il controllo e la fiducia che ha l'utente verso la Smart Home.
Il progetto ha ricevuto un finanziamento di 4'754'875 euro da parte dell'Unione Europea, distribuiti tra vari istituti appartenenti a diverse nazioni, e ha come coordinatore il Consiglio Nazionale delle Ricerche italiano. Ha avuto ufficialmente inizio il 1° ottobre 2020 e la data di conclusione del progetto è prevista per il 30 settembre 2023.
A questo progetto contribuiscono varie realtà, e il suo consorzio comprende attori di spicco nelle industrie IoT, di telecomunicazioni e di cybersecurity, nonché istituti accademici e di ricerca.

### 3.2.1 Architettura

Il sistema SIFIS, come illustrato in *Figura* 3.3 è composto da due componenti principali:

- un software framework che utilizza protocolli di comunicazione sicuri e che permette di gestire e far rispettare le funzionalità relative alla sicurezza, di

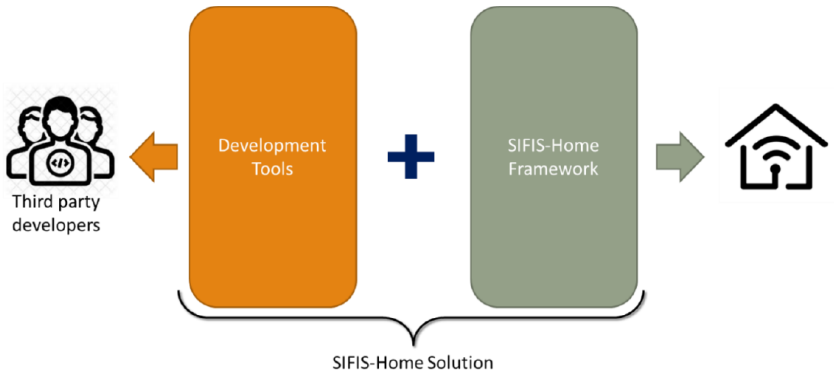



Figura 3.3: Componenti principali di SIFIS-HOME

svolgere attività di processamento dei dati in maniera rispettosa della privacy, e di garantire comunicazioni sicure in maniera resiliente, facile ed efficiente

- un insieme di strumenti e librerie (un toolkit) che permette agli sviluppatori software di progettare applicazioni che sfruttino il potenziale dell'architettura SIFIS per implementare funzionalità relative alla sicurezza nelle loro applicazioni

All'interno della Smart Home sono presenti due tipologie di devices:

- **Smart Devices**: dispositivi con buone capacità computazionali e dotati di un sistema operativo in cui poter installare applicazioni terze: sono la base dell'architettura in quanto hanno installato il framework SIFIS. Un esempio di dispositivo Smart è un PC o un frigorifero 'intelligente'.
- **Not So Smart Devices(NSSD)**: dispositivi che seppur in grado comunicare tra di loro e con alcune funzionalità computazionali, presentano una ridotta potenza di calcolo e non possono essere personalizzati installando applicazioni terze. Un esempio di dispositivo Not-So-Smart è una lampadina o un sensore 'intelligenti'.

Gli Smart Devices sono quindi la parte centrale dell'architettura, gestendo operazioni e scambiando messaggi, mentre i NSSD vengono considerati dispositivi periferici

sotto il diretto controllo dei Smart Device e hanno il compito di interagire col mondo fisico attraverso i sensori e attuatori.
L'architettura del framework SIFIS è divisa in 4 parti fondamentali, ognuna di queste interagisce con un elemento differente dell'ambiente: SIFIS-Home Smart Devices Framework, SIFIS-Home Application Framework, SIFIS-Home NSDD Framework e SIFIS-Home Cloud Framework. Questi elementi sono stati progettati per seguire il design dei microservizi[1], che favorisce flessibilità e modularità.

### SIFIS-Home Smart Devices Framework

SIFIS-Home Smart Device Framework è l'insieme di componenti software installati all'interno dei Smart Devices. Questo framework è diviso in macrocomponenti ognuno dei quali offre differenti funzionalità:

- **SIFIS-Home API Gateway**: questo componente include un insieme di API di alto livello e ha lo scopo di interfacciare il dispositivo con applicazioni esterne
- **Secure Lifecycle Manager**: è il gestore del ciclo di vita del framework, regolando la presenza e il comportamento degli Smart Devices e delle applicazioni. In particolare, questa componente svolge la funzione di gestire la registrazione di nuovi dispositivi e gestire l'installazione e la disinstallazione di applicazioni terze
- **NSSD Manager**: è la componente responsabile della gestione dei Not So Smart Devices, premettendo la ricerca di questi dispositivi e il loro controllo
- **Application Toolboxes**: è l'insieme di componenti software che svolge funzioni di analisi dei dati, anonimizzazione dei dati e rinforzo delle policy (cioè

[1] l'architettura dei microservizi struttura l'applicazione in un insieme di servizi che sono indipendenti tra di loro e connessi in maniera minima, riducendo le dipendenza presenti nel codice

un sistema che valuta le richieste di azioni e servizi, cercando quelle che vanno contro le policy di utilizzo, privacy e sicurezza definite dall'amministratore)

- **Secure Communication Layer**: si occupa di gestire il sicuro scambio di messaggi tra i vari devices
- **Proactive Security Management Layer**: questa componente gestisce automaticamente tutte le funzioni relative alla gestione della sicurezza, come il rilevamento di anomalie e intrusioni, attivando le appropriate misure per fermare e mitigare tali comportamenti. È diviso in 3 sottocomponenti: Monitors (identifica le minacce per la sicurezza), Self-healing (rileva, analizza e aggiusta le problematiche relative ai devices e alla rete) e Distributed Trust (in caso di un device compromesso, non essendo un sistema centralizzato, questa componente permette di svolgere un sistema di votazione tra i restanti devices)
- **DHT Manager**: permette una comunicazione tra le varie parti del software attraverso un approccio publish/subscribe
- **VPN Manager**: permette la connessione al server VPN di SIFIS-Home. In questo modo è possibile accedere allo smart device dall'esterno dell'abitazione

### SIFIS-Home Application Framework

SIFIS-Home Application Framework è l'insieme di componenti software installati in un dispositivo mobile (smartphone) usati per controllare la Smart Home. Questa componente è il principale punto d'accesso al sistema per l'utente ed è per questo dotata di un GUI (Graphic User Interface). Anche questa componente è divisa in vari moduli:

- **Home**: lo scopo principale del modulo è di fornire all'utente una visione d'insieme del sistema, permettendogli di osservare lo stato generale senza dover navigare oltre

- **Device Management**: permette di vedere la lista di devices (sia Smart che Not So Smart) consentendog di aggiungerli e rimuoverli dalla lista, nonché di rinominarli e gestire la possibilità di invio o meno di allarmi

- **Alarms/Logs**: questa componente offre la possibilità di mostrare all'utente gli allarmi generati dai vari dispositivi

- **Impostazioni**: Diviso in impostazioni degli utenti e impostazioni del sistema. Con le impostazioni degli utenti è possibile vedere la lista di utenti della Smart Home, creandone di nuovi o rimuovendoli, nonché di gestire i propri dati biometrici. Le impostazioni del sistema permettono di gestire le varie policies che controllano in senso generale il sistema

- **Application Launcher**: da questa componente l'utente può visualizzare le applicazioni installate. Può inoltre installarne di nuove e aggiornare o rimuovere quelle già presenti

- **Input Collection**: utilizzato per permettere all'utente di fornire input al dispositivo, che possono essere di tipo vocale o per mezzo della fotocamera

### SIFIS-Home NSDD Framework

SIFIS-Home Not-So-Smart-Device Framework è l'insieme delle componenti software presenti nei dispositivi Not-So-Smart. Queste componenti sono divise in 2 gruppi distinti, il Bootstrap Manager e il Device API Manager. Il Bootstrap Manager si occupa di raccogliere tutte le informazioni che servono al dispositivo per connettersi alla rete dell'abitazione. Il Device API Manager offre una serie di API che permettono di controllare il dispositivo.

#### SIFIS-Home Cloud Framework

SIFIS-Home Cloud Framework è l'insieme delle componenti e applicazioni software presenti nel cloud SIFIS-Home e che hanno lo scopo principale di permettere all'utente di controllare l'abitazione da remoto. Queste sono divise in 4 unità principali. Marketplace è una componente webservice che fornisce una serie di API che permettono di gestire le applicazioni terze installabili negli Smart Devices; per ogni applicazione è riportato l'URL per il download nonché il livello di sicurezza assegnato. Inoltre, Marketplace permette a uno sviluppatore esterno di caricare una sua applicazione. La seconda unità di questo framework è il server VPN Server che permette di accedere ai dispositivi anche da remoto. SIFIS-Yggio, la terza componente, ha il compito di fornire delle API che siano rispettose degli standard FIWARE[2]. Infine, Home Registration Manager mette a disposizione un'interfaccia da cui è possibile inizializzare una casa provvista del framework SIFIS-Home.

### 3.2.2 Aspetti etici e legali

Come riportato nei documenti relativi al progetto, le persone che lavorano in SIFIS-Home sono consapevoli del fatto che lo sviluppo di un sistema IoT per l'abitazione va a toccare aspetti molto privati e intimi della vita di una persona, rendendo necessaria un'elevata attenzione per gli aspetti etici e legali.

#### GDPR

Naturalmente, il primo aspetto legale da considerare è il rispetto del GDPR. Il sistema processa i dati personali delle persone all'interno dell'abitazione ed è quindi necessario prendere le adeguate misure per essere rispettosi del GDPR, come ad

[2]FIWARE è un'iniziativa europea che, al fine di aumentare la competitività europea in ambito ICT, mette a disposizione un'infrastruttura tecnologia open source e un insieme di specifiche di comunicazione basate su standard open

esempio progettando i servizi in modo da seguire i principi di privacy by design e by default. In particolare, si è deciso di creare una dashboard che faciliti il rispetto dei principi del regolamento, permettendo all'utente di esercitare i suoi diritti e rendendo più facile la comunicazione dei vari attori in gioco. Lo sviluppo di questa dashboard è stato il lavoro principale di questa tesi e verrà analizzato nel dettaglio nel prossimo capitolo.

### Analisi etiche

Tutte le azioni svolte all'interno della piattaforma SIFIS-Home devono avere l'obiettivo di proteggere i valori e la dignità dell'essere umano. A tale scopo, la protezione dei diritti fondamentali dell'uomo ha la priorità rispetto alla protezione degli interessi dei singoli attori, come le aziende, le pubbliche autorità e altri. SIFIS si pone quindi come obiettivo la protezione di questi diritti, concentrandosi in particolare sulle seguenti questioni:

- **Privacy**: Tra i diritti che SIFIS-Home vuole salvaguardare c'è sicuramente il diritto alla privacy. SIFIS si impegna a sviluppare applicazioni e servizi che rispettino il principio di privacy by design e by default e implementino le appropriate misure per garantire un livello di sicurezza dei dati adeguato
- **Sicurezza fisica**: Un'altra priorità considerata è la sicurezza fisica: i dispositivi IoT interagiscono col mondo esterno compiendo azioni che potrebbero causare danni a persone o cose; è quindi importante sviluppare ed utilizzare tecnologie ed applicazioni che rispettino il principio di safety by design e by default
- **Discriminazioni**: Molte applicazioni attuali fanno utilizzo di tecniche di Machine Learning. Queste applicazioni possono essere sviluppate da terzi ed installate negli Smart Devices degli utenti. Tuttavia, queste tecnologie, e non solo queste, spesso hanno dei bias che inficiano il risultato finale portando a

delle discriminazioni[3]. SIFIS quindi si impegna ad utilizzare applicazioni e servizi privi di questi bias e che non portino a discriminazioni

- **Controllo dell'utente**: L'utilizzo di tecnologie IoT, soprattutto in un ambiente come l'abitazione domestica, può avere un impatto importante sulla vita di un individuo. Fondamentale è quindi garantire la libertà di scelta della persona riguardo a come utilizzare queste tecnologie e a chi dare accesso ai dati personali che producono. Per garantire questa libertà è fondamentale che i sistemi SIFIS permettano all'utente di compiere una scelta informata e consapevole, dandogli il pieno controllo dei suoi dati e permettendogli di scegliere se e a chi fornirne l'accesso

### Software libero

Oltre agli aspetti appena citati, non si può non considerare il contributo che ha il software libero in questo discorso. Per software libero s'intende un software distribuito sotto i termini di una licenza che, contrariamente al software proprietario, ne concede lo studio, l'utilizzo, la modifica e la redistribuzione. In particolare, secondo la Free Software Foundation (un'organizzazione non a scopo di lucro fondata da Richard Stallman, uno dei principali esponenti del movimento del software libero) un software è considerato libero se garantisce 4 libertà fondamentali [55]: libertà di eseguire il programma per qualsiasi scopo; libertà di studiare come funziona il programma e di modificarlo in base alle proprie necessità; libertà di ridistribuire copie del programma in modo da aiutare il prossimo; libertà di migliorare il programma e di distribuirne pubblicamente i miglioramenti, in modo tale che tutta la

[3]Uno degli esempi più noti di bias è quello relativo al word embedding, un metodo che rappresenta le parole come vettori, permettendo di compiere operazioni matematiche per misurare la loro vicinanza semantica. Questo permette anche di compiere analogie, ad esempio componendo la frase 'L'uomo è re, la donna è X', si otteneva automaticamente il risultato X=regina. Tuttavia, si è osservato come utilizzando frasi come 'L'uomo è ingegnere, la donna è X', il risultato era X=casalinga, dimostrando come, a causa dei dati utilizzati per l'allenamento, il sistema avesse dei pregiudizi sessisti.

comunità ne tragga beneficio.

SIFIS-Home si impegna ad implementare e distribuire tecnologie e applicazioni basate sul software libero in quanto aiutano a far rispettare i diritti descritti precedentemente. Se si utilizzano queste tecnologie, infatti, gli utenti hanno la possibilità di analizzarne il funzionamento e in parte modificarlo. Inoltre, si permette la promozione della collaborazione e contribuzione tra gli sviluppatori, portando a un miglioramento di queste tecnologie.

# Capitolo 4

# Privacy Dashboard

La tesi si pone l'obiettivo di sviluppare una Web App che, interagendo col framework SIFIS-Home, faciliti la gestione del GDPR nelle applicazioni IoT per Smart Home. In particolare, l'app, oltre a garantire una facile e veloce comunicazione tra gli attori in gioco, implementa un meccanismo per permettere all'utente di applicare in maniera intuitiva e informata i propri diritti e al responsabile di rispettare in maniera semplice i propri doveri.

## 4.1 Stato dell'arte

Prima di procedere allo sviluppo della Web App si è indagato sullo stato dell'arte relativo a tecnologie simili: cioè a quei software che facilitano il rispetto del GDPR o forniscono un maggiore controllo dei dati personali dell'interessato. Di seguito un breve riassunto dei software considerati più significativi.

#### Cookie Script

Cookie Script contiene un insieme di strumenti utilizzabili dagli sviluppatori per fare in modo che il loro sito web rispetti vari normative, tra cui il GDPR. Cookie Script permette di analizzare i cookies utilizzati da un sito web (anche cookies di terzi),

fornirne una descrizione e classificarli in 5 categorie: 'Strictly Necessary', 'Performance', 'Targeting', 'Functionality' e 'Unclassified'. La versione a pagamento del programma permette di bloccare degli specifici cookies, fornisce uno strumento per compilare il Privacy Notice e permette di gestire le preferenze degli utenti relative a un sito web.

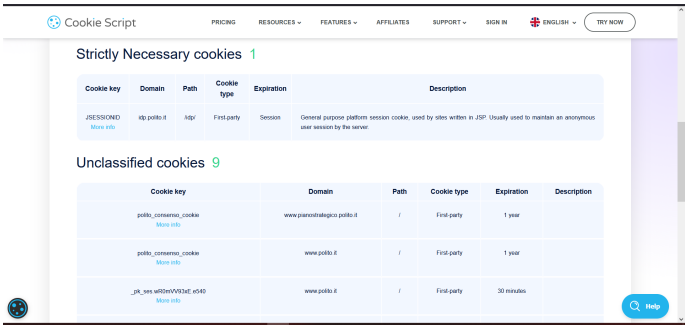



Figura 4.1: Analisi dei cookies fornita da CookieScript per il sito del Politecnico di Torino

### GDPR-Self assessment di BayLDA

La BayLDA (Bayerisches Landesamt für Datenschutzaufsicht), la Data Protection Authority dello stato tedesco della Baviera, ha messo a disposizione un questionario che permette di capire il livello di rispetto del GDPR da parte di un'azienda.

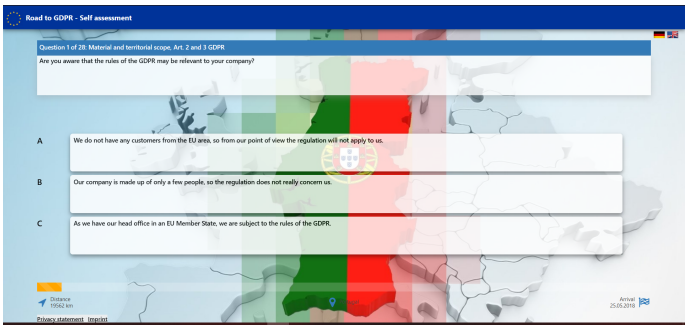



Figura 4.2: Esempio di una domanda del questionario di Bayla

### Webbkoll

Webbkoll è uno strumento che permette di analizzare alcuni livelli di sicurezza di un sito web. Tra le varie verifiche che compie sono presenti il controllo che il sito utilizzi https di default anziché http, l'analisi del Content Security Policy [1], l'analisi dei cookie utilizzati e in generale il controllo delle misure atte ad aumentare la privacy degli utenti (ad esempio controlla se alcune informazioni sono passate a siti terzi).

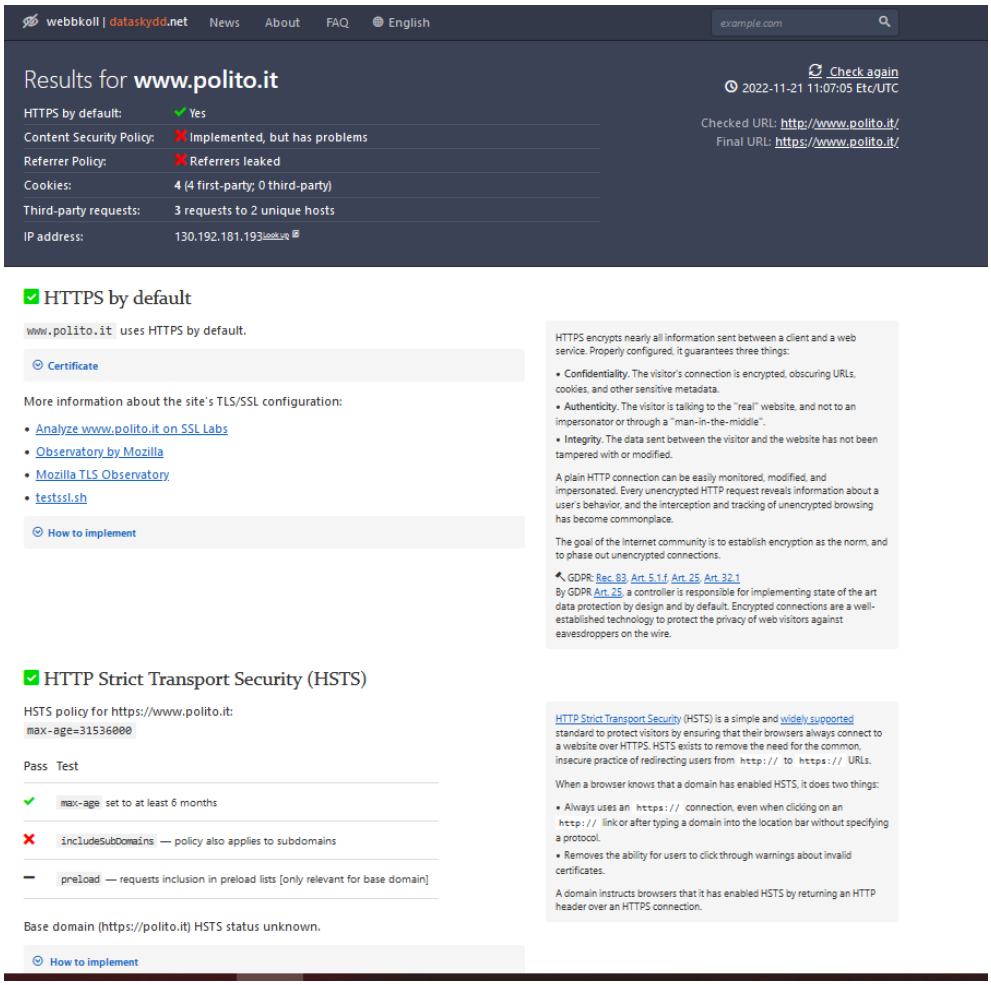



Figura 4.3: Analisi del sito del Politecnico di Torino da parte di Webbkoll

[1] Il Content Security Policy è un livello di sicurezza addizionale che aiuta a rilevare e mitigare alcuni tipi di attacchi tra cui attacchi di Data Injection e Cross Site Scripting (XSS)

#### EDPS' Website Evidence Collector

EDPS' Website Evidence Collector è uno strumento open source che analizza e salva in un formato YAML o HTML, in modo che siano visionabili dall'utente, le informazioni che un sito web salva e trasferisce quando lo si visita.

#### CNIL's open source PIA software

Questo strumento, sviluppato dal CNIL (Commission nationale de l'informatique et des libertés), l'autorità francese incaricata di assicurare l'applicazione della legge sulla tutela dei dati personali, aiuta i Data Controller a scrivere il Privacy Impact Assessment.

## 4.2 Tecnologie utilizzate

Per lavorare sulla Web App si è deciso di avvalersi dell'aiuto di Vaadin, uno strumento open source che facilita lo sviluppo di queste applicazioni in Java. Uno dei principali vantaggi di Vaadin, e quello maggiormente sfruttato in questo progetto, è quello di gestire in maniera semplice la parte grafica dell'applicazione, utilizzando oggetti Java per creare elementi normalmente instanziabili utilizzando linguaggio HTML e CSS. Questa funzionalità permette di gestire questi elementi ed effettuare azioni su di essi in maniera più organica e integrata alla logica dell'applicazione, personalizzandoli comunque attraverso alcuni file CSS, seppur in maniera più ridotta rispetto al solito.
Vaadin inoltre utilizza al suo interno anche Spring Security, un framework del progetto Spring che consente di gestire in modo semplice e trasparente l'autenticazione e l'autorizzazione degli utenti che accedono ad una applicazione web. Spring Security, infatti, è stato utilizzato nell'ambito di questo progetto appunto per gestire la

registrazione di nuovi utenti, il loro log-in e log-out e controllare in maniera semplice quello che potevano o non potevano fare. Inoltre, è stato utilizzato anche per altre azioni relative alla sicurezza come la cifratura delle password degli utenti.

## 4.3 Functional Requirements

Prima di procedere allo sviluppo dell'applicazione, sono stati identificati i Functional Requirements (Requisiti funzionali)

| ID | DESCRIZIONE |
|---|---|
| **FR1** | **Gestione degli utenti** |
| FR1.1 | Permette di utilizzare la dashboard in qualità di Data Subject (interessato), Data Controller (titolare del trattamento) o Data Protection Officer (DPO), fornendo funzionalità differenti |
| FR1.2 | Permette di gestire la registrazione di un nuovo utente |
| FR1.3 | Permette di gestire il log-in dell'utente, accedendo alla sua pagina personale e gestendo i suoi personali contatti e applicazioni |
| FR1.4 | Permette di gestire le informazioni dell'utente come il cambio di mail o di password |
| FR1.5 | Permette di effettuare il log-out dell'utente dall'applicazione |
| **FR2** | **Gestione dei contatti** |
| FR2.1 | Permette all'utente di vedere la lista dei contatti disponibili in base alle applicazioni utilizzate. (ad esempio: il Data Subject potrà vedere i contatti dei Data Controllers e DPOs associati alle applicazioni installate) |
| FR2.2 | Permette di vedere le informazioni dei contatti (indirizzo mail se inserito, ruolo del contatto, app associate al contatto) |

| ID | DESCRIZIONE |
|---|---|
| FR2.3 | Permette l'invio e la ricezione di messaggi dall'utente ad un contatto |
| **FR3** | **Privacy Notice** |
| FR3.1 | Permette al Data Subject di visionare i privacy notice delle applicazioni |
| FR3.2 | Permette al Data Subject di scaricare i privacy notice delle applicazioni |
| FR3.3 | Permette al Data Controller o al DPO di scrivere da zero il privacy notice per le applicazioni a loro associate |
| FR3.4 | Permette al Data Controller o al DPO di scrivere, attraverso una sezione precompilata e provvista di esempi, i privacy notice per le applicazioni a loro associate |
| FR3.5 | Permette al Data Controller o al DPO di caricare e associare alle applicazioni un privacy notice già compilato |
| FR3.6 | Permette al Data Controller o al DPO di modificare i privacy notice delle applicazioni a loro associate |
| **FR4** | **Valutazione del rispetto del GDPR** |
| FR4.1 | Permette al Data Subject di vedere la valutazione relativa al rispetto del GDPR delle applicazioni (sistema a semaforo: rosso, arancione, verde) |
| FR4.2 | Permette al Data Controller e al DPO di effettuare il questionario relativo al rispetto del GDPR da parte delle applicazioni |
| FR4.3 | Permette al Data Controller e al DPO di modificare le risposte date a un precedente questionario relativo al rispetto del GDPR da parte delle applicazioni |

| ID | DESCRIZIONE |
|---|---|
| FR4.4 | Una volta concluso il questionario relativo al rispetto del GDPR da parte dell'applicazione, permette di visionare un riassunto in cui vengono riportati gli aspetti critici dell'applicazione |
| **FR5** | **Diritti e Doveri** |
| FR5.1 | Permette al Data Subject di vedere che diritti possiede |
| FR5.1.1 | Diritto 'Data Portability': avere accesso ai propri dati personali |
| FR5.1.2 | Diritto 'Withdraw a consent': diritto di ritirare un consenso precedentemente dato |
| FR5.1.3 | Diritto 'Ask information': diritto di chiedere informazioni, come ad esempio il periodo di mantenimento dei dati, lo scopo del processamento dei dati o il fatto che i dati vengano inviati a terzi |
| FR5.1.4 | Diritto 'Complain': diritto di inviare un reclamo all'autorità competente |
| FR5.1.5 | Diritto 'Erase': diritto di eliminare delle informazioni personali |
| FR5.2 | Permette al Data Subject di inviare una richiesta di applicazione di un suo diritto a chi di competenza |
| FR5.3 | Permette al Data Subject di visualizzare la lista delle richieste inviate, dividendole tra quelle già risolte e quelle ancora da prendere in carico |
| FR5.4 | Permette al Data Controller e al DPO di ricevere le richieste di applicazione dei diritti da parte dei Data Subject |
| FR5.5 | Permette al Data Controller e al DPO di visualizzare la lista delle richieste ricevute, dividendole tra quelle già risolte e quelle ancora da prendere in carico |
| FR5.6 | Permette al Data Controller e al DPO di rispondere alle richieste dei Data Subjects, permettendo di scrivere una risposta |

| ID | DESCRIZIONE |
|---|---|
| FR5.7 | Permette al Data Controller e al DPO di cambiare lo stato delle richieste del Data Subject da 'ancora da prendere in carico' a 'risolta' e viceversa |
| **FR6** | **Gestione notifiche** |
| FR6.1 | Invio di notifiche e ricezione di notifiche nel caso in cui vengano compiute certe azioni |
| FR6.1.1 | Invio messaggio: notifica al contatto a cui è stato inviato |
| FR6.1.2 | Compilazione o modifica Privacy Notice: notifica a tutti i Data Subjects associati alla relativa app |
| FR6.1.3 | Compilazione o modifica questionario per il rispetto del GDPR: notifica a tutti i Data Subjects associati alla relativa app |
| FR6.1.4 | Invio richiesta di applicazione un diritto: notifica a Data Controller e DPO responsabili |
| FR6.1.5 | Risposta alla richiesta o modifica stato richiesta: notifica al Data Subject che aveva inviato la richiesta |
| **FR7** | **Navigazione tra le sezioni della Web App** |
| FR7.1 | Vari elementi nella pagina permettono il passaggio tra le varie schermate in maniera semplice e veloce |
| **FR8** | **Gestione API per comunicare con altre applicazioni** |

## 4.4 Ruoli

L'applicazione permette di gestire 3 tipologie di utenti differenti: i Data Subjects, i Data Controllers e i Data Protection Officers (DPOs). Nel momento della registrazione l'utente avrà la possibilità di scegliere uno dei tre ruoli, che non sarà più possibile cambiare. La differenza tra i ruoli sta nell'accessibilità alle varie parti dell'applicazione e nelle funzioni permesse: la maggior parte delle pagine sono

accessibili a chiunque abbia effettuato il log in ma ce ne sono alcune che sono specifiche o per i Data Subject o per i Data Controllers e DPOs. Inoltre, anche nelle pagine accessibili a tutti, alcune funzioni sono permesse soltanto ad uno specifico ruolo. Infine, un'altra differenza importante tra i vari ruoli sta nella visibilità delle informazioni disponibili: mentre le informazioni dei Data Subject sono private e, ad esempio, nessun utente a parte il titolare può vedere l'elenco delle proprie applicazioni installate, per i Data Controllers e i DPOs alcune informazioni sono accessibili a chiunque permettendo, ad esempio, che chiunque possa verificare di quali applicazioni è responsabile un certo DPO.

## 4.5 Architettura

Dal punto di vista architetturale, la Web App è divisa in varie parti:

- Una parte relativa alle pagine visibili dall'utente durante la sua navigazione nell'app e che verranno discusse nel dettaglio più avanti
- Una parte relativa alla gestione dei vari oggetti che vengono salvati nel database. Questa sezione si occupa sia di astrarre gli oggetti base, come gli utenti e le applicazioni IoT installate, che di gestire le operazioni effettuabili sul database. Per implementarla, si è sfruttato il framework Spring andando ad avvalersi della specifica JPA: ogni tabella presente nel database è andata quindi a collegarsi univocamente con un oggetto java, e sono state create delle interfacce 'repository' per specificare le azioni da compiere sul database
- Una parte che permette la corretta comunicazione tra le varie pagine dell'applicazione, permettendo una navigazione fluida e consentendo il passaggio di informazioni ritenute utili tra le varie pagine
- Una parte relativa alla sicurezza. In questa sezione viene utilizzato Spring Security personalizzando la gestione dell'autenticazione e dell'autorizzazione

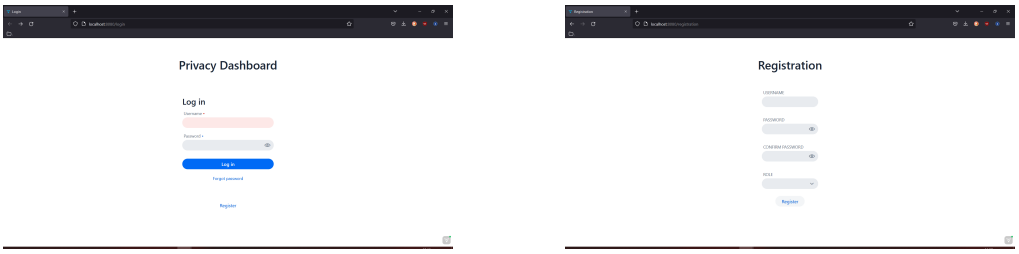
- Una parte relativa alla comunicazione con il framework di SIFIS-Home e con applicazioni esterne. Qui vengono utilizzate delle Rest API per scambiare informazioni tra i due sistemi

Si andrà ora ad analizzare più approfonditamente le varie pagine visitabili dall'utente quando utilizza la Web App.

### 4.5.1 Log In

Questa è la prima pagina che viene presentata all'utente quando utilizza l'applicazione e serve a permettergli di effettuare il log-in o di registrarsi per la prima volta. Ogni username è univoco, perciò nel momento della registrazione è necessario utilizzarne uno non ancora utilizzato. L'utente dovrà inoltre scegliere il ruolo che svolgerà (Data Subject, Data Controller o Data Protection Officer) e non sarà possibile modificare la scelta in futuro né avere ruoli differenti per differenti applicazioni (se un utente fosse un Data Controller per un'applicazione e volesse usare la Web App come Data Subject per un'altra applicazione dovrà creare due account differenti). Ci sono infine alcune restrizioni per la scelta dello username e della password: il primo deve avere una lunghezza di almeno 5 caratteri mentre la seconda deve avercela di almeno 8 caratteri. Naturalmente le password sono salvate solo dopo essere state cifrate e la funzione di hashing utilizzata, sfruttando le funzionalità di Spring Security, è BCrypt[2].

[2]BCrypt è un algoritmo a chiave simmetrica a blocchi che utilizza un salt (differente per ogni cifratura) producendo un hash di 184 bit. È interessante specificare che in questo algoritmo è possibile scegliere un parametro costo, che all'aumentare del valore rende più lungo il tempo necessario per fare l'hash, permettendo una migliore protezione contro attacchi di forza bruta.




(a) Schermata di log-in (b) Schermata per la registrazione

Figura 4.4: Schermate di log in e registrazione

### 4.5.2 Home

Una volta effettuato il log-in, l'utente può accedere liberamente a tutte le pagine in cui ha l'autorizzazione, a partire dalla pagina principale, la Home. In questa schermata, l'utente può velocemente accedere alle principali pagine a cui è autorizzato. Come si può notare nelle *Figure* 4.5 e 4.6, la maggior parte delle pagine accessibili sono uguali sia per Data Subjects che per Data Controllers/DPOs ad eccezione di due: i Data Subjects possono accedere alla pagina *Pending Requests*, da cui è possibile visionare le richieste di attuazione dei diritti non ancora prese in carico, mentre i Data Controllers/DPOs possono accedere alla pagina *Questionnaire*, da cui è possibile compilare il questionario per verificare il livello di rispetto per il GDPR che ha una certa applicazione. Con l'aiuto della *Figura* 4.5 si andrà ora ad analizzare il layout dell'applicazione stessa, comune a quasi tutte le pagine.

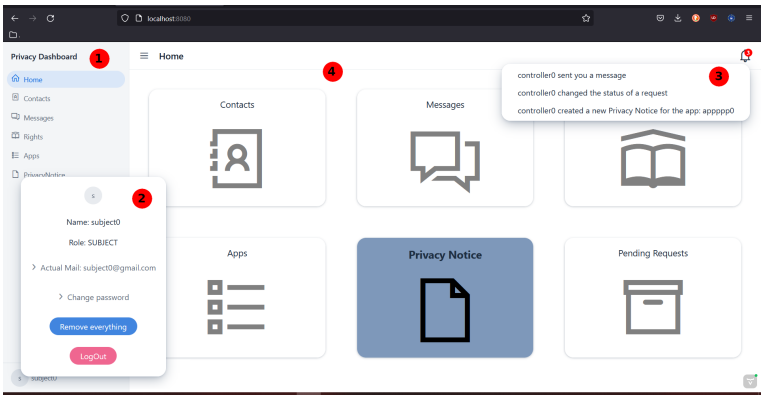



Figura 4.5: Pagina di Home per Subject

1. **Menu a tendina**: Sulla sinistra è presente un menu a tendina che può essere visibile in base alle necessità dell'utente (in *Figura* 4.6 il menu non è visibile) e da cui è possibile navigare facilmente tra le varie pagine dell'applicazione
2. **Profilo**: Cliccando in basso a sinistra comparirà un piccolo spazio dedicato alla modifica del profilo dell'utente. Da qui è possibile modificare e-mail e password nonché effettuare il log out. Esclusivamente per i Data Subjects è presente anche il pulsante "*Remove everything*" che permette all'utente di inviare una richiesta per l'eliminazione di ogni suo dato personale da tutte le applicazioni in suo possesso
3. **Notifiche**: In alto a destra è presente il simbolo delle notifiche, una campana con un numero sovrimpresso che rappresenta il numero delle notifiche non lette dall'utente. Cliccando il simbolo comparirà uno spazio con un riassunto delle notifiche. Cliccando su ciascuna notifica si verrà reindirizzati nell'apposita sezione (se ad esempio era una notifica di un nuovo messaggio, si verrà reindirizzati nella pagina della conversazione in cui è presente quel messaggio)
4. **Pagina**: Mentre gli elementi sopracitati rimangono immutati durante la navigazione tra le varie pagine dell'applicazione, la parte centrale della schermata varia in base alla pagina visitata. Nel caso della Home, vengono rappresentati sei riquadri da cui è possibile navigare tra le varie pagine dell'applicazione

### 4.5.3 Contacts

In questa pagina è presente l'elenco di tutti i contatti dell'utente, specificandone il nome, il ruolo e la mail. Per ciascun contatto sono inoltre presenti un link per navigare nella pagina della conversazione, nonché le app che questo ha in comune con l'utente (cliccando sopra nome dell'applicazione è possibile navigare nella pagina relativa all'applicazione).

I contatti vengono considerati nel seguente modo: in caso di Data Controller/DPO,

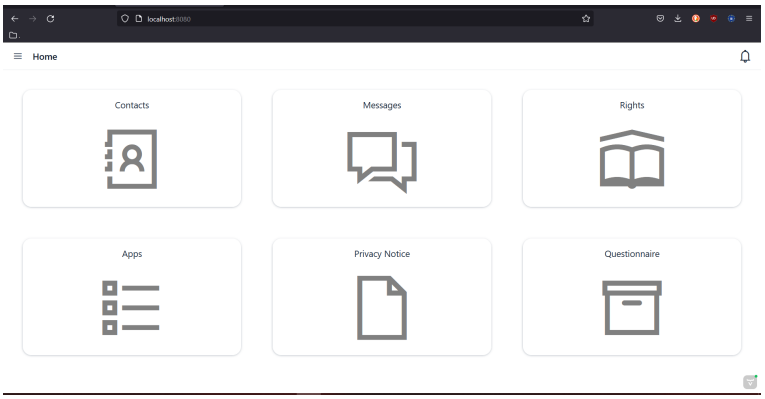



Figura 4.6: Pagina di Home per Controller

qualsiasi persona, indipendentemente dal ruolo che ha, che possiede almeno un'applicazione in comune con l'utente viene considerato un suo contatto. Per i Data Subjects, invece, vengono considerati contatti solo le persone che hanno in comune un'applicazione ma che non sono anche loro dei Data Subjects. Ciò permette di rendere più facile la comunicazione verso i Data Controllers/DPO (sia tra di loro che tra i Data Subjects), ma anche di impedire l'accesso di informazioni a chi non ne ha strettamente necessità (un Data Subject non ha bisogno di conoscere l'indirizzo mail di un altro Data Subject ma potrebbe aver bisogno di quello di un DPO)

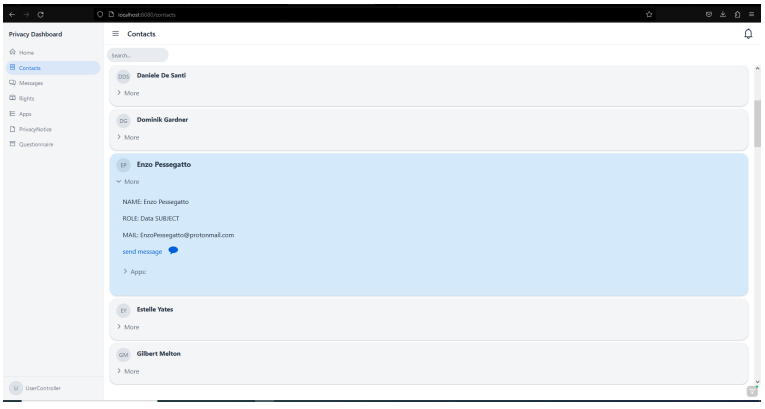
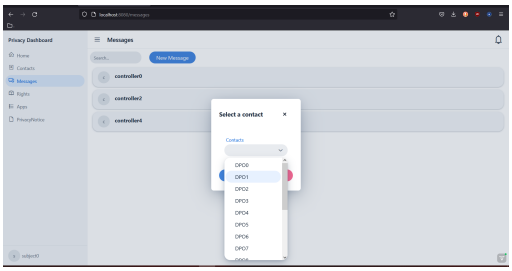


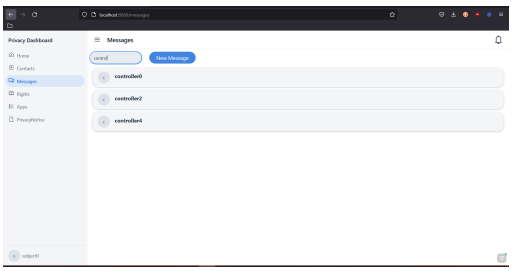

Figura 4.7: Pagina dei contatti

### 4.5.4 Messages

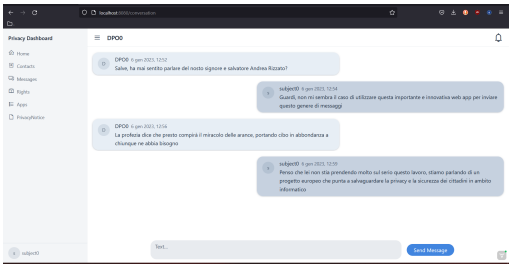
Questa pagina contiene la lista delle conversazioni tra gli utenti. Nella parte superiore della schermata, oltre all'area di testo per ricercare un contatto, è presente un pulsante per un nuovo messaggio che farà comparire una sezione, come si può vedere in *Figura* 4.8a, in cui si può selezionare un contatto per cominciare una nuova conversazione. Cliccando invece in una delle schede dei contatti, come quelle in *Figura* 4.8b, si verrà reindirizzati nella pagina della singola conversazione (*Figura* 4.8c) da cui si possono vedere i messaggi scambiati e inviarne di nuovi



(a) Inizializzazione nuovo messaggio



(b) Pagina dei messaggi



(c) Conversazione singola

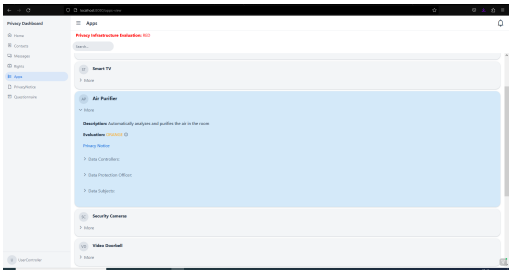
Figura 4.8: Pagina dei messaggi

### 4.5.5 Apps

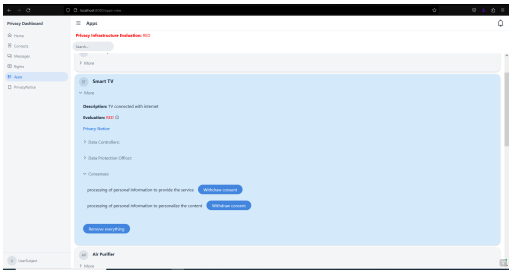
Da questa pagina l'utente può visionare l'elenco di tutte le applicazioni in suo possesso. Per ognuna di queste, come visionabile nella *Figura* 4.9a, è presente una descrizione dell'app (fornita dal Controller o dal DPO della stessa), il voto ricevuto nel questionario per verificare il rispetto del GDPR (i voti sono Verde, Giallo,

Rosso), un link per il Privacy Notice dell'applicazione e infine la lista dei contatti che possiedono l'applicazione.

Come si può notare in *Figura* 4.9b, per i Data Subject al posto della lista dei contatti Data Subject che utilizzano l'applicazione (come specificato nella sezione dei Contacts, due Subjects non sono considerati tra loro contatti) è presente la lista dei consensi che l'utente ha dato per quell'applicazione, permettendo di ritirarli facilmente premendo l'apposito pulsante, e il pulsante "*Remove Everything*" che invia la richiesta di rimozione di tutti i dati personali relativi a quell'applicazione



(a) Pagina delle App per Controller/DPO



(b) Pagina delle App per Subject

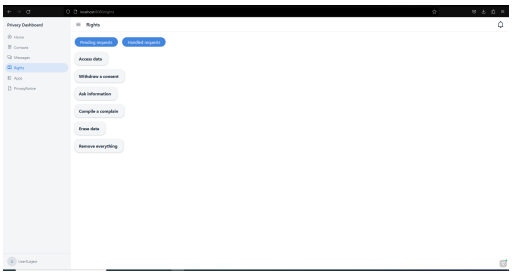
Figura 4.9: Pagina delle App

### 4.5.6 Rights

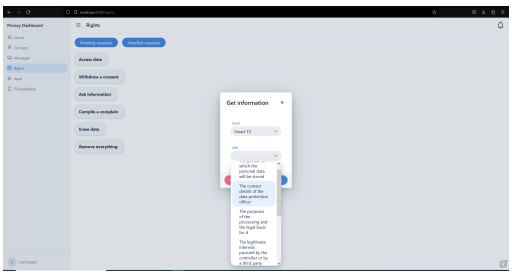
Questa pagina presenta delle importanti differenze tra quella relativa al Data Subject e quella relativa al Data Controller/DPO.

#### Data Subject

In questa pagina(*Figura* 4.10a) i Data Subject potranno compiere una delle azioni più importanti disponibili nella piattaforma: fare una richiesta per usufruire di un loro diritto. Qui l'utente potrà selezionare una delle cinque opzioni presenti nella schermata e che porterà all'apertura di uno specifico form da compilare inserendo i dettagli dell'azione (*Figura* 4.10b):



(a) Pagina dei diritti per Subject



(b) Finestra dopo aver selezionato un'opzione

Figura 4.10: Pagine dei diritti per Subject

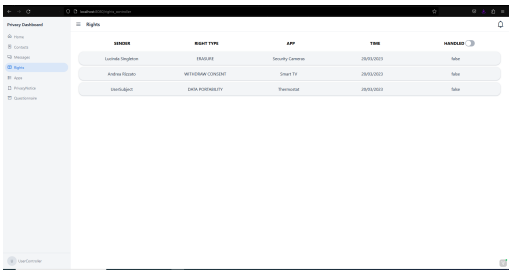
- **Access data**: Da qui l'utente seleziona un'applicazione da cui chiedere di accedere ai suoi dati personali in un formato aperto e comunemente utilizzato (XML, JSON...)
- **Withdraw a consent**: L'utente seleziona l'applicazione e il consenso che vuole ritirare
- **Ask information**: Da qui l'utente può richiedere delle specifiche informazioni riguardanti l'utilizzo dei suoi dati personali da parte di un'applicazione. L'utente può scrivere quale informazione vuole ottenere o può selezionare una delle scelte prestabilite che includono il periodo di mantenimento dei dati, i destinatari dei dati, gli interessi legittimi del Data Controller o delle terze parti e altre
- **Compile a complain**: Da qui l'utente può scrivere un reclamo relativo ad una specifica applicazione all'autorità di supervisione
- **Erase data**: L'utente, dopo aver selezionato un'applicazione, indica quali dei suoi dati personali desidera che vengano eliminati. Viene ricordato, inoltre, che un'azione simile può essere compiuta al di fuori da questa pagina attraverso i pulsanti "*Remove everything*" che inviano una richiesta di rimozione di tutti i dati personali dell'utente

Una volta conclusa questa procedura verrà inviata una richiesta al responsabile dell'applicazione che riceverà una notifica e sarà suo compito gestire tale richiesta.

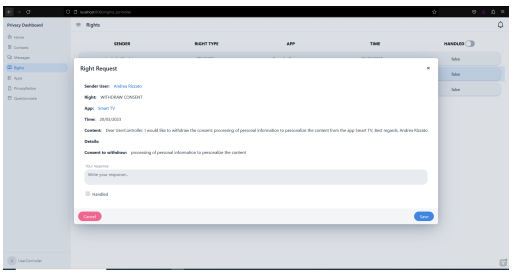
Infine, nella schermata, attraverso i due pulsanti in alto, si può accedere alla lista di richieste già prese in carico (*Handled requests*) e di quelle ancora in lavorazione (*Pending requests*) che si presenteranno in una maniera simile alla schermata del Data Controller/DPO (*Figura* 4.11a).

### Data Controller/DPO

La pagina per i Data Controllers/DPO (*Figura* 4.11a) presenta la lista delle richieste di applicazione dei diritti ricevute dai Data Subjects, permettendo di filtrare tra quelle già soddisfatte e quelle ancora da completare.
Selezionando una specifica richiesta si aprirà una finestra (*Figura* 4.11b) da cui saranno visibili i dettagli. Da questa finestra, inoltre, oltre a cambiare lo stato della richiesta da 'in corso' a 'completata' e viceversa, l'utente potrà anche rispondere direttamente al Data Subject, fornendogli ad esempio le informazioni che aveva richiesto (in caso la richiesta fosse relativa all'invio di informazioni) oppure la risposta dell'autorità di supervisione (in caso di reclamo a quest'ultima).



(a) Pagina dei diritti per Controller/DPO

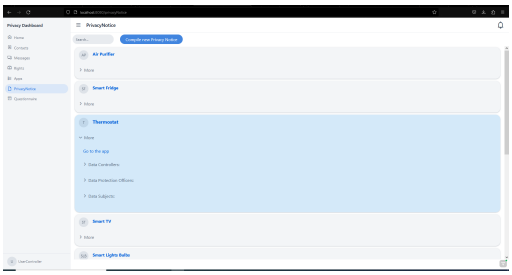


(b) Descrizione di una singola richiestae

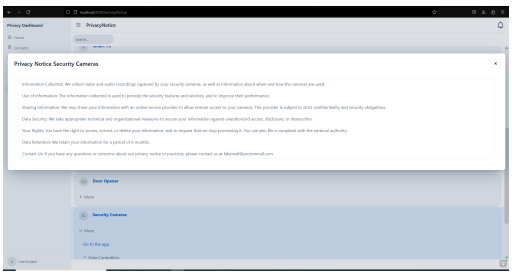
Figura 4.11: Pagine dei diritti per Controller/DPO

## 4.5.7 Privacy Notice

Come riportato precedentemente (Capitolo 1, *Doveri del titolare del trattamento*), il Privacy Notice è un documento in cui sono riportate importanti informazioni relative al processamento dei dati. La pagina principale(*Figura* 4.12a) contiene, sia



(a) Lista delle Privacy Notice



(b) Specifica Privacy Notice per Subject

Figura 4.12: Pagina dei Privacy Notice

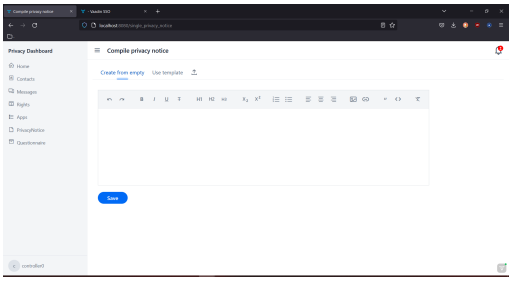
per il Data Subject che per il Data Controller, la lista delle applicazioni insieme alle relative informazioni, mentre solo per il Data Controller/DPO è presente la possibilità di compilare un nuovo Privacy Notice.

Selezionando una specifica applicazione, si potranno compiere azioni differenti in base al ruolo che si ha: per il Data Subject si aprirà un'area di testo (*Figura* 4.12b) in cui sarà possibile visionare il documento specifico dell'applicazione; per il Data Controller/DPO invece sarà possibile visionare e modificare il documento (o crearne uno nuovo nel caso non ce ne fosse uno già presente). In quest'ultimo caso l'utente può utilizzare tre modalità distinte:

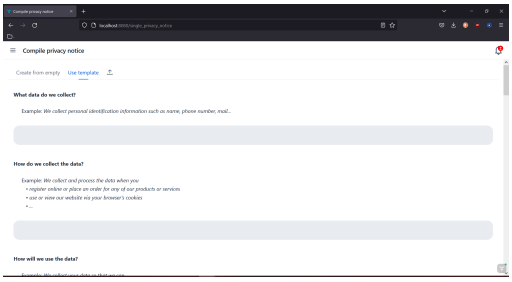
- **Compilazione da zero**: Qui l'utente potrà compilare liberamente il documento, senza seguire nessuna linea guida
- **Compilazione da template**: Qui l'utente sarà guidato nella compilazione del documento rispondendo a delle specifiche domande provviste di esempi di possibile risposta. Per la scelta delle domande da utilizzare si è fatto affidamento al template per la compilazione del Privacy Notice fornito dal sito GDPR.eu[3]

[3]GDPR.eu è una risorsa, fondata dall'Unione Europea attraverso il progetto Horizon 2020, lo stesso di SIFIS-Home, che fornisce aiuto a organizzazione e individui riguardo i vari aspetti del GDPR

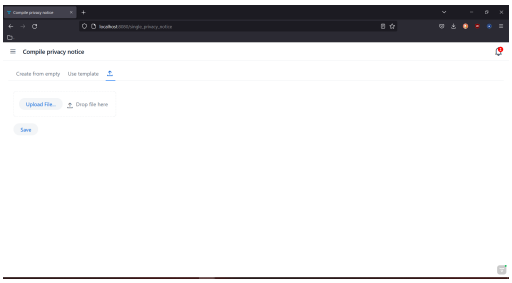
- **Caricamento del file**: Da questa sezione sarà possibile caricare un file contente il testo direttamente nella piattaforma. Al momento, tuttavia, questa funzionalità non è ancora attiva



(a) Compilazione da zero



(b) Compilazione da template



(c) Caricamento del file

Figura 4.13: Schermate delle varie possibilità per la compilazione del Privacy Notice

### 4.5.8 Questionnaire

Questa pagina è riservata ai Data Controllers e ai DPOs e permette di effettuare il questionario per capire quanto un'applicazione è rispettosa del GDPR. La pagina, mostrata in *Figura* 4.14, è composta dalla lista di applicazioni di cui è già stato effettuato il questionario, colorando la scritta per evidenziarne il voto ottenuto, dalla sezione di testo per cercare una specifica applicazione e dal pulsante che permette di effettuare una nuova valutazione. Quando viene selezionata un'applicazione, si viene reindirizzati nella pagina del questionario vera e propria (*Figura* 4.15). Ogni risposta riceve una classificazione basata sui colori (il sistema è equivalente a quello

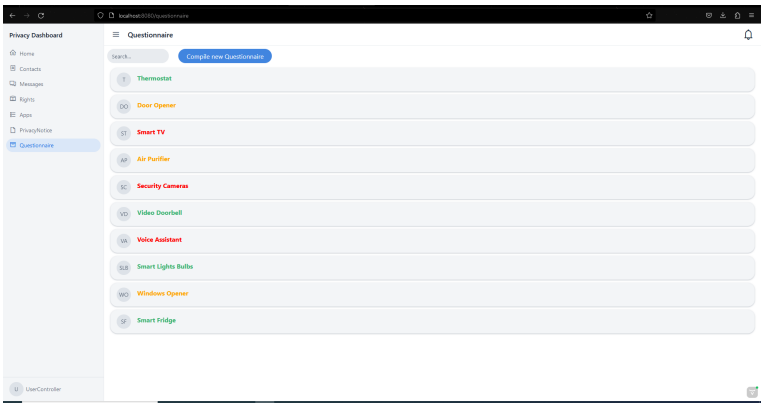



Figura 4.14: Pagina dei questionari

semaforico): verde indica che la risposta soddisfa completamente il GDPR, arancione significa che la risposta non soddisfa a pieno i principi del GDPR mentre si utilizza il rosso nel caso in cui la risposta vada contro i principi del GDPR.
Le domande sono divise in 3 sezioni, più una riassuntiva:

- **Personal Data**: qui sono presenti domande relative al processamento dei dati personali degli utenti, concentrandosi sul luogo in cui vengono salvati, il periodo di mantenimento e la facilità con cui i proprietari possono accederne
- **Security**: in questa sezione vengono effettuate domande relative alla sicurezza dell'applicazione, come ad esempio l'uso di crittografia, di pseudonomizzazione dei dati e di altre misure di sicurezza
- **Tests and certifications**: in questa sezione viene chiesto se sono stati effettuati dei test o se si è in possesso di certificati volti ad accertare i livelli di controllo dell'utente e di sicurezza dell'applicazione
- **Riassunto**: come ultima sezione è presente un riepilogo delle risposte date, specificandone il numero per categoria(verde, arancione, rosso)(*Figura* 4.16)

Le domande sono state selezionate cercando di coprire in maniera sufficientemente sintetica ma esaustiva tutti i principi base del GDPR, utilizzando anche il

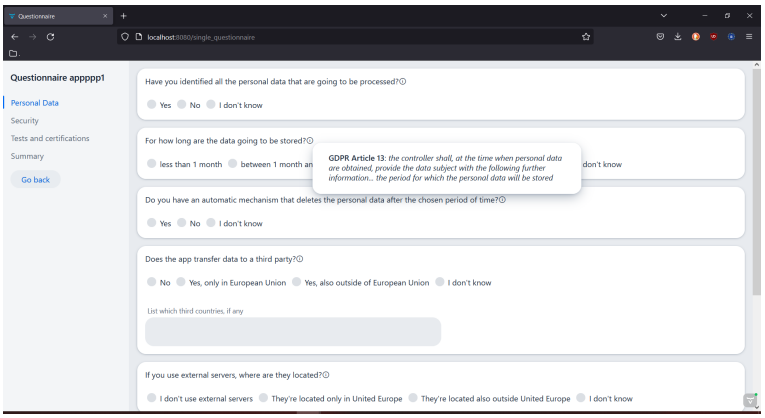



Figura 4.15: Questionario per una applicazione

supporto di una documentazione fornita dal CNIL [4] in cui vengono fornite delle linee guida per sviluppare software rispettando il GDPR.

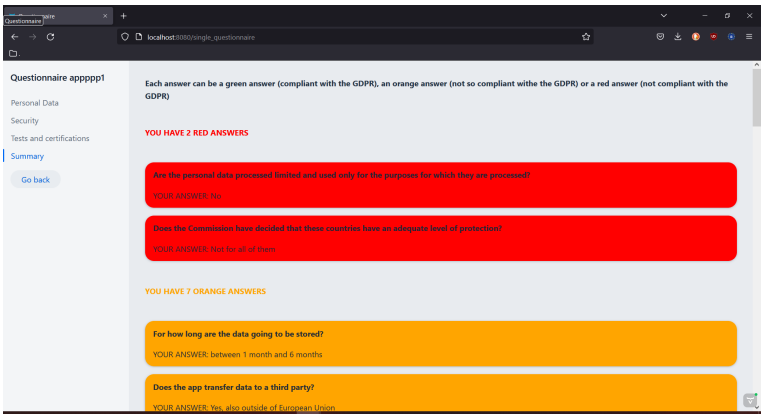



Figura 4.16: Pagina riassuntiva del questionario

Effettuare il questionario offre una duplice utilità: in primo luogo permette al responsabile di farsi un'idea del livello che raggiunge la sua applicazione in quest'ambito, nonché di considerare aspetti che magari prima aveva trascurato; in

[4] il CNIL, Commission nationale de l'informatique et des libertés, è un'autorità amministrativa indipendente francese incaricata di assicurare l'applicazione della legge sulla tutela dei dati personali nei casi in cui si effettuino raccolte, archiviazioni ed elaborazioni di dati personali. Il sito utilizzato è il seguente: https://www.cnil.fr/en/gdpr-developers-guide

secondo luogo, fornisce al Data Subject uno strumento chiaro e semplice per verificare il livello di sicurezza e di privacy delle app da lui scaricate permettendogli di compiere una scelta più consapevole.

### 4.5.9 APIs

Oltre alle schermate navigabili dall'utente una volta effettuato il log in, questa applicazione mette a disposizione una serie di funzioni API che permettono la comunicazione con applicazioni terze. In particolare, queste funzioni sono state pensate per comunicare con il framework SIFIS, non escludendo però la comunicazione con ulteriori fonti, permettendo quindi ad un variegato insieme di applicazioni di beneficiare di questa funzionalità.
Per utilizzare queste API è necessario essere autenticati dal sistema e per fare ciò è stato deciso di utilizzare http basic authentication, che codifica le credenziali dell'utente che deve essere identificato. Questo metodo, tuttavia, non gestisce la cifratura del messaggio ed è quindi necessario utilizzarlo solo sfruttando un canale sicuro, ad esempio inviando la richiesta attraverso HTTPS.
Le API permettono di compiere qualsiasi azione disponibile tra le funzionalità dell'applicazione e, per creare una corrispondenza diretta con la navigazione standard dell'app, si è deciso di classificare le API in base alle pagine a cui fanno riferimento. Tutte le chiamate iniziano con il prefisso *api/*, seguito dal gruppo a cui fanno riferimento (ad esempio, una funzione api che vuole ottenere le informazioni di un'applicazione avrà il seguente prefisso *api/app*).
Per alcune funzioni, oltre alla necessaria autenticazione, sono presenti ulteriori limitazioni e solo alcuni utenti possono accedere a determinate informazioni. Ad esempio, la funzione *api/privacynotice/add* aggiunge un documento del privacy notice ad una specifica applicazione; solamente chi è identificato come controller o DPO di quell'applicazione potrà effettuare l'azione.

# Capitolo 5

# Conclusioni

## 5.1 Risultati ottenuti

Uno dei benefici principali che fornisce questo strumento è la possibilità di mettere in comunicazione i Data Subjects e i Data Controllers/DPOs senza che sia necessario inserire informazioni personali, in quanto la comunicazione avviene senza utilizzare indirizzi mail, il cui inserimento come dato è assolutamente opzionale.
Per i Data Subject, questo strumento acquisisce un valore particolarmente elevato perché dà informazioni sui propri diritti e permette di applicarli in maniera semplice e immediata, senza necessità di conoscenze particolari: una delle questioni più spinose in questi ambiti è la mancata conoscenza da parte degli utenti delle varie regolamentazioni in vigore e l'inconsapevolezza di avere il diritto ad effettuare determinate azioni. Con questa applicazione si cerca in parte di sanare questa problematica, dando all'utente una lista dei diritti che possiede e permettendogli, in poche azioni, di inviare la richiesta di applicazione del diritto.
Anche per i Data Controllers e i DPOs questo strumento può rivelarsi particolarmente comodo in quanto gestisce, in una singola piattaforma, la maggior parte dei doveri che devono svolgere. Nella Web App, infatti, l'utente può gestire tutte le applicazioni di cui è responsabile, può interagire con i Data Subject, compilare il

Privacy Notice e tenere sotto controllo le varie richieste di applicazioni dei diritti tutto nella stessa applicazione, in maniera semplice e intuitiva.

## 5.2 Lavori futuri

Questa è una prima versione della Web App e in futuro potrà essere migliorata aggiungendo ulteriori funzionalità.
Primo fra tutti c'è la gestione del caricamento e scaricamento dei vari documenti in diversi formati, in particolare il Privacy Notice e il documento, in formato XML e JSON, contenente i dati personali appartenenti all'utente di una specifica applicazione.
Un altro aspetto che potrebbe aggiungere valore alla Web App sarebbe l'aggiunta di una pagina relativa alla compilazione e alla visione del Privacy Impact Assessment, un processo volto ad aiutare il Data Controller ad analizzare, identificare e minimizzare in maniera sistematica i rischi relativi alla protezione dei dati.
Inoltre, non è stato possibile far interagire la Web App con il framework SIFIS-Home, e non è quindi stato possibile testare il modo e la maniera in cui nella pratica le due piattaforme interagiscono tra di loro; un obiettivo futuro è senza dubbio verificare questa interazione, il cui risultato porterà probabilmente alla progettazione di nuovi e migliori meccanismi della Web App, o a delle funzioni API differenti.
Infine, con minimi cambiamenti, la Web App può essere molto versatile e utilizzata per differenti applicazioni oltre che per SIFIS-Home; sarebbe interessante vedere a quali piattaforme può essere estesa (ad esempio una piattaforma per gestire le applicazioni di uno smartphone) e come renderla più generica in modo da poter essere utilizzata negli ambiti più disparati.

# Bibliografia


[1] A. F. Westin, *Privacy and freedom*. Ig Publishing, 2018.

[2] Aristotele, *Politica*.

[3] W. Jaeger, *Pideia III*. Bompiani, 2003.

[4] H. Arendt, *Vita activa*. University of Chicago Press, 1958.

[5] S. Iaselli, Michele e Gorla, *Storia della privacy*. Lex Et Ars, 2015.

[6] J. B. Calhoun, "Population density and social pathology," *Scientific American*, 1962.

[7] "David attenborough: zoos should use peepholes to respect gorillas' privacy," 2016.

[8] "Animals need digital privacy too," 2020.

[9] "Dr. geertz's paper was delivered informally at a seminar on privacy conducted by members of the center for advanced study in the behavioral sciences, stanford, calif., in 1959.,"

[10] M. B. Nimmer, "The right of publicity," *Law and Contemporary Problems*, 1954.

[11] "Letter from roscoe pound to william chilton (1916), quoted in a. mason, brandeis: A free man's life, p. 70 (1956), cited by glancy 1979, p. 1.,"

[12] "Privacy in colonial new england,"

[13] "Stati per densità di popolazione." `https://it.wikipedia.org/wiki/Stati_per_densit%C3%A0_di_popolazione`, 2022.

[14] "Dichiarazione universale dei diritti dell'uomo," 1948.

[15] "Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali," 1950.

[16] "Pub.l. 93–579, 88 stat. 1896, enacted december 31, 1974, 5 u.s.c. § 552a," 1974.

[17] "Health insurance portability and accountability act," 1996.

[18] "Children's online privacy protection act," 1998.

[19] "Sentenza n. 34 anno 1973 corte costituzionale repubblica italiana," 1973.

[20] "Guidelines on the protection of privacy and transborder flows of personal data the organization for economic co-operation and development," 1981.

[21] G. ufficiale delle Comunità europee, "Direttiva 95/46/ce del parlamento europeo e del consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati," 1995.

[22] G. ufficiale delle Comunità europee, "Direttiva 97/66/ce del parlamento europeo e del consiglio del 15 dicembre 1997 sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni," 1997.

[23] G. ufficiale delle Comunità europee, "Direttiva 2002/58/ce del parlamento europeo e del consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunica- zioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche)," 2002.

[24] "Data protection directive 95/46/ec," 1995.

[25]

[26]

[27] "Caso bonus covid: il garante privacy sanziona l'inps per 300mila euro." `https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9556927`, 2021-03-09.

[28] "Causa google." `https://www.bbc.com/news/technology-46944696`, 2019.

[29] "Causa whatsapp." https://www.publico.es/internacional/irlanda-multa-225-millones-whatsapp-violar-normativa-europea-proteccion-datos.html, 2021.

[30] "Causa amazon." https://techcrunch.com/2021/07/30/eu-hits-amazon-with-record-breaking-887m-gdpr-fine-over-data-misuse/?guccounter=1&guce_referrer=aHR0cHM6Ly9lbi53aWtpcGVkaWEub3JnLw&guce_referrer_sig=AQAAAC4bDrDmr2QzqaAMbnKiwQ1F7LqFpYV5UVadDRS0JuGE1lUtj9mxlrVQp 2021.

[31] "Schrems 1." https://www.lastampa.it/tecnologia/2015/10/20/news/la-sentenza-della-corte-ue-sulla-privacy-spiegata-in-10-punti-1.3521, 2015.

[32] "privacy shield." https://ec.europa.eu/newsroom/article29/items, 2016.

[33] "Cloud act." https://edps.europa.eu/sites/edp/files/publication/19-07-10_edpb_edps_cloudact_annex_en.pdf, 2019.

[34] "Schrems 2." https://archive.epic.org/privacy/intl/dpc-v-facebook/cjeu/, 2021.

[35] R. 7452, "Architectural considerations in smart object networking." https://tools.ietf.org/html/rfc7452, 2015.

[36] ITU, "Overview of the internet of things." http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=Y.2060, 2012.

[37] "Impact of internet of things(iot) on the business economy – 2022 trends." https://sumatosoft.com/blog/impact-of-internet-of-things-iot-on-the-business-economy-2022-trends, 2022.

[38] "Machine to machine." https://en.wikipedia.org/wiki/Machine_to_machine, 2015.

[39] "The internet toaster." http://www.livinginternet.com/i/ia_myths_toast.htm, 2000.

[40] I. A. Board, "Architectural considerations in smart object networking." `http://www.livinginternet.com/i/ia_myths_toast.htm`, 2015.

[41] I. A. Board, "Architectural considerations in smart object networking." `https://www.rfc-editor.org/rfc/rfc7452.txt`, 2015.

[42] "What does iot need to thrive? interoperability comes into play." `https://pandorafms.com/blog/interoperability-in-iot/`, 2021.

[43] I. Society, "The internet of things: An overview understanding the issues and challenges of a more connected world," 2015.

[44] "Large ddos attacks cause outages at twitter, spotify, and other sites." `https://techcrunch.com/2016/10/21/many-sites-including-twitter-and-spotify-suffering-outage/`, 2016.

[45] "We need to save the internet from the internet of things." `https://www.schneier.com/essays/archives/2016/10/we_need_to_save_the_.html`, 2016.

[46] "Top cyber attacks on iot devices in 2021." `https://firedome.io/blog/top-cyber-attacks-on-iot-devices-in-2021/`, 2021.

[47] "Eight crazy hacks: The worst and weirdest data breaches of 2015." `https://securityintelligence.com/eight-crazy-hacks-the-worst-and-weirdest-data-breaches-of-2015/`, 2015.

[48] X. Liu, "Security and privacy challenges for internet-of-things and fog computing," *Wireless Communications and Mobile Computing*, 2018.

[49] P. N. Howard, *Pax Technica, How the Internet of Things May Set Us Free or Lock Us Up*. Yale University Press, 2015.

[50] P.-P. Verbeek, *Moralizing Technology: Understanding and Designing the Morality of Things*. The University of Chicago Press, 2011.

[51] "Invasion of the data snatchers big data and the internet of things

means the surveillance of everything." https://tomdispatch.com/crump-and-harwood-the-net-closes-around-us/, 2014.

[52] "Statista." https://www.statista.com/outlook/dmo/smart-home/worldwide?currency=EUR, 2022.

[53] "Smart home technologies in europe: A critical review of concepts, benefits, risks and policies,"

[54] S. Zuboff, *Il capitalismo della sorveglianza*. NY: Profile Books, 2019.

[55] "Cos'è il software libero?." https://www.gnu.org/philosophy/free-sw.it.html, 2022.