UNIVERSITÀ
DEGLI STUDI
DI PADOVA

DIPARTIMENTO
DI INGEGNERIA

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

CORSO DI LAUREA IN INGEGNERIA INFORMATICA

Analisi dei problemi di privacy connessi con il protocollo OCPI in prospettiva del GDPR

Relatore: Prof. Mauro Migliardi

Laureando: Alessandro Longo

ANNO ACCADEMICO 2022 – 2023

Data di laurea 20 Luglio 2022

Indice

Abstract

Quello della mobilità elettrica è un settore che sta rapidamente crescendo e, in quanto tale, molte aziende stanno facendo la loro comparsa nel mercato, trasformando il settore da una realtà piccola e contenuta, ad una più complessa e, soprattutto, molto interconnessa.

Questo perché la presenza di molti attori con ruoli diversi o anche solo di compagnie competitor che svolgono lo stesso ruolo nel mercato necessità di ulteriori attori con un ruolo di comunicazione, affinché si possa creare un network che funzioni adeguatamente. Il protocollo OCPI in esame, già abbastanza diffuso nel settore, più specificatamente nell'ambito della ricarica dei veicoli elettrici, si propone di svolgere questo ruolo.

L'obiettivo di questo studio è valutare, in prospettiva del GDPR, ovvero delle normative europee attualmente vigenti sulla privacy, se il protocollo in questione rispetti i diritti degli utenti, oppure se in esso siano presenti delle inadempienze.

L'importanza di questo argomento è data dal fatto che, sebbene il protocollo OCPI abbia un ruolo marginale nell'ecosistema della mobilità elettrica e i dati e le informazioni sensibili che esso manipola ed utilizza siano limitati, nondimeno è fondamentale che lo sviluppo di questo settore proceda in maniera trasparente ed etica, rispettando le normative vigenti in Europa e con un chiaro focus anche sulla sicurezza, tanto nella protezione dagli attacchi esterni, quanto nella salvaguardia dei dati sensibili degli utenti che ne utilizzano i servizi.

Capitolo 1

Introduzione

1.1 L'informatizzazione del mondo della mobilità

Il mondo della mobilità elettrica è perennemente in crescita e, a questo punto, è abbastanza chiaro che rappresenterà il futuro della nuova generazione di automobili.
Questo nuovo tipo di mobilità, però, non è caratterizzata dal solo fatto di essere elettrica ma anche dalla maggiore connettività e informatizzazione. I veicoli, infatti, sono sempre più spesso dotati di sistemi informatici interni che permettono loro di comunicare sia tra di loro, che con le infrastrutture stradali.

Questo cambiamento porterà in futuro ad un gran numero di vantaggi e, si prevede, avrà un grande impatto sul mondo della mobilità. Grazie a queste nuove tecnologie i conducenti potranno avere informazioni in tempo reale, quali la disponibilità di parcheggi, i limiti di velocità, le condizioni del traffico e meteorologiche e molto altro. In più, tra i vantaggi sopraelencati, è bene sottolineare che la connettività tra veicoli ed infrastrutture, quali semafori, centri di gestione del traffico o cartelli a messaggio variabile, incrementerà notevolmente anche la sicurezza stradale**,** l'efficienza del traffico e il comfort di guida**.** Si può parlare, quindi, di una tecnologia che, oltre a facilitare le condizioni di guida quotidiane, incrementerà anche il livello di sicurezza degli automobilisti.

Questo processo di evoluzione del mondo della mobilità elettrica – e non solo – è ormai in corso da molti anni e la crescita nel tempo è stata notevole; l'informatica ha iniziato a far parte di questo mondo in maniera evidente già nel momento in cui, nelle auto, è stato inserito il navigatore satellitare integrato, il quale era, a tutti gli effetti, un primo "computer di bordo". Guardando al futuro, invece, e tentando di prevedere la direzione di quello che si prospetta come un moto di crescita non ancora terminato, si può intravedere che il settore si spinge sempre più in là nella connettività e nell'informatizzazione, ad esempio nei progetti di auto senza pilota. Per questa ragione, analizzare questo fenomeno, i cambiamenti che comporta e le problematiche che può celare, non è solamente utile per il nostro presente ma lo è anche per anticipare quello che sarà un probabile futuro, in luce del percorso che è stato fatto fino a qui e della direzione che è possibile intravedere osservando i progetti di avanguardia dei colossi del settore.

Tutti i cambiamenti, però, hanno un costo e, se da una parte ci sono i vantaggi portati da questo avanzamento tecnologico, dall'altra la maggior informatizzazione porta a delle nuove problematiche da affrontare nell'ambito della sicurezza; molto più complesse rispetto a quelle riguardanti la mera sicurezza del veicolo, che fino ad ora erano l'unica preoccupazione in tal senso.

La presenza di sistemi informatici, infatti, crea una nuova superfice di attacco per potenziali criminali, i quali potrebbero, ad esempio, installare dei programmi malevoli nel veicolo sfruttando eventuali vulnerabilità del sistema e traendone così vantaggi illeciti. Questo però non è il solo possibile tipo di attacco: nel momento in cui il mondo dell'informatica viene integrato a quello dell'automobile, infatti, sono molte di più le minacce alla sicurezza che si affacciano sul settore, alcune già ben note e affrontate da anni negli ambiti di cybersecurity, altre invece completamente nuove che emergeranno, sfruttando situazioni e vulnerabilità uniche, prodotte dall'unione di questi due settori.

Tra tutte le possibili vulnerabilità da proteggere, evitare che i dati sensibili dell'automobilista vengano compromessi è sicuramente una delle sfide più ardue. Questo perché la possibilità di sottrarre tali dati non si limita al contatto con il veicolo ma, proprio per via della connettività che si persegue, ciò che maggiormente viaggia tra le varie entità interconnesse sono i dati, e durante uno qualsiasi di questi passaggi, se non dovessero essere adeguatamente protetti, questi potrebbero venir attaccati e sottratti.

1.2 Il settore della mobilità elettrica

Andando ora ad approfondire più specificatamente il mondo della mobilità elettrica, possiamo dire che si tratta di un settore relativamente nuovo e, come anticipato nel paragrafo precedente, in rapida crescita ed espansione. Per questa ragione anche i modelli di business sono ancora in via di sviluppo e ciò rende il settore una realtà molto sfaccettata, che coinvolge numerosi attori i quali, a loro volta, sono correlati tra di loro in un complesso intreccio.

Tra questi attori ci sono ovviamente diverse società e aziende sia nate dalle necessità di questo settore, come i *Charge Point Operators* (CPO) e gli *e-Mobility Service Providers* (eMSP), sia già esistenti ma con ambiti correlati come i roaming hubs e gli attori del settore dell'energia, tra i quali, ad esempio, gli operatori della griglia elettrica e i produttori di energia.
Oltre a queste aziende anche i governi nazionali hanno implementato una serie di politiche ad influenzare il settore, queste includono la definizione di obiettivi nazionali, le campagne d'informazioni e le sovvenzioni, sia in forma di incentivi all'acquisto di automobili elettriche,

sia in forma di finanziamenti atti alla costruzione di un'infrastruttura di stazioni di ricarica pubblica.

Per finire, nuove tendenze emergono in continuazione e danno origine a proposte di business che possono partire anche dai singoli utenti o da piccole compagnie come, ad esempio, i servizi di car sharing o la possibilità di ottenere un profitto restituendo alla griglia elettrica corrente che si era precedentemente acquistato ("*vehicle-to-grid technology*").

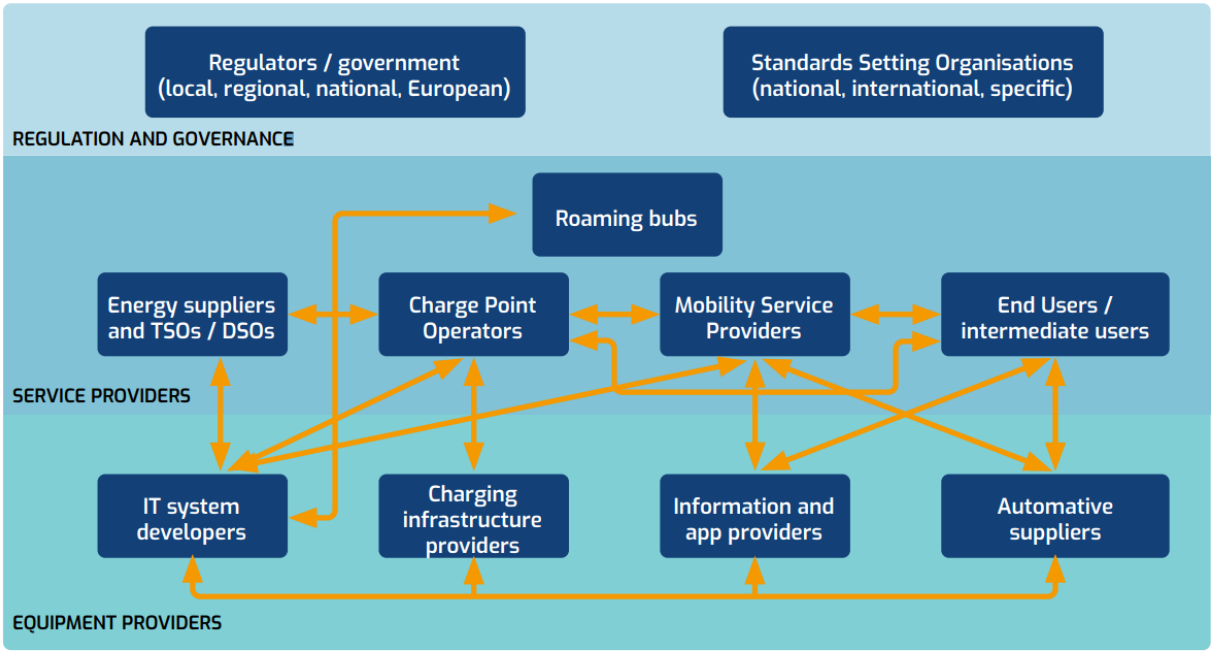


Figura 1 Figure di mercato coinvolte nell'ecosistema dei veicoli elettrici e le loro connessioni

1.3 La ricarica dei veicoli elettrici

In un settore così vasto e complesso sono moltissimi gli aspetti sui quali ci si potrebbe concentrare e che si potrebbero approfondire. Un aspetto fondamentale però, poiché imprescindibile e immutabile dai modelli di business e da come questi evolveranno in futuro, è quello della ricarica dei mezzi elettrici. Questo perché, perlomeno in questo momento storico, è difficile immaginare i veicoli elettrici potranno mai fare a meno di essere caricati.

Ebbene, costruire un'infrastruttura di ricarica efficiente e al contempo di facile utilizzo richiede che tutti gli attori coinvolti comunichino e scambino dati relativi alle operazioni di ricarica. Ciò è particolarmente vero quando si cerca di ottenere un roaming completo ("*seamless roaming*"), il che significa una situazione nella quale un utente può caricare il proprio veicolo elettrico in qualsiasi stazione di ricarica pubblica, indipendentemente da quale CPO gestisce quella stazione di ricarica e indipendentemente dall'eMSP selezionato dall'utente per i servizi di mobilità e pagamento. Ad aggiungersi all'esigenza già impegnativa di mettere in contatto e

abilitare alla comunicazione così tante entità differenti, gli sviluppi futuri previsti richiederanno l'ingresso di sempre più attori da collegare a questo network. Ad esempio, in vista dell'avvento dei sistemi di ricarica intelligente, gli attori del settore della ricarica (ad ora principalmente CPO, eMSP e roaming hub) dovranno interagire con gli attori del settore energetico, come gli operatori di rete e i produttori di energia. Infine, il roaming transnazionale di veicoli elettrici richiederà anche agli attori di diversi paesi di comunicare tra loro.

In uno scenario come questo i protocolli sono cruciali per garantire una comunicazione efficiente tra tutte le parti coinvolte. Sono proprio questi, infatti, che si occupano sia di regolare e delimitare le informazioni che possono essere condivise, sia di consentire e gestire le comunicazioni tra gli attori.

1.3.1 "I fondamentali" della ricarica nella mobilità elettrica

Per l'analisi più approfondita che si farà in seguito, il cui soggetto principale è il protocollo OCPI, è necessario prima di tutto presentare quelli che sono gli attori principali con cui questo interagisce e qual è la loro funzione.

CPO:

I CPO collegano e operano le stazioni di ricarica intelligenti per veicoli elettrici. Solitamente si tratta anche di coloro che si occupano della costruzione e dell'installazione delle stazioni di ricarica.

Il loro principale lavoro, in sintesi, è quello di fornire la tecnologia necessaria per mantenere l'infrastruttura funzionante e fare in modo che le stazioni di ricarica possano interagire con il mondo esterno: ciò include tutto, da una semplice richiesta di "addebito iniziale" posta dall'utente finale, fino a complessi scambi di comandi di domanda e risposta alla griglia elettrica. Le due facce del lavoro del CPO quindi sono quella hardware, che ne include l'installazione, l'assicurarsi che la stazione di ricarica funzioni in maniera corretta e che il servizio sia sempre attivo, gestendo anche eventuali malfunzionamenti; e quella software che gestisce, ad esempio, la diagnostica, la manutenzione, l'impostazione dei prezzi e la gestione dei dati dei POI (Point of Interest).

Aldilà del suo ruolo, un Charge Point Operator (CPO) è una società che gestisce un certo numero di punti di ricarica e fornisce valore collegando i dispositivi di ricarica intelligenti agli eMSP.

Le società, in base alle loro esigenze, possono essere molto diverse tra di loro, di conseguenza a volte un CPO possiede anche l'infrastruttura (la “colonnina” vera e propria), altre volte fornisce semplicemente la tecnologia per permettere ad essa di operare.

La società che possiede il CPO certe volte potrebbe anche possedere un servizio di eMSP, in tal caso la comunicazione tra le due entità sarebbe enormemente semplificata. Ad ogni modo, la società in questione potrebbe voler consentire l’accesso ai punti di ricarica anche ad altri utenti, che utilizzano differenti eMSP. Se invece la società che possiede il CPO non gestisce nessun tipo di servizio eMSP, essa si deve affidare completamente a quest’ultimi per fornire l’accesso alle loro stazioni di ricarica.
Tranne in alcuni particolari casi, perciò, è spesso necessario stabilire un contatto tra CPO e eMSP non appartenenti alla stessa azienda, questa evenienza è possibile e viene realizzata grazie all’utilizzo di reti in roaming.

eMSP:

Gli eMSP forniscono all'utente finale l'accesso alle stazioni di ricarica per veicoli elettrici e ne permettono un facile utilizzo, solitamente tramite l’impiego di un’applicazione.

Il loro lavoro è quello di aiutare i conducenti di veicoli elettrici a trovare le stazioni di ricarica, avviare eventi di ricarica e pagare. Sta a loro, inoltre, gestire la parte tecnica della transazione, dai metodi di pagamento, all’adeguamento delle tariffe e l’addebito in tempo reale.

Anche in questo caso, un e-Mobility Service Provider (eMSP) è un'azienda che offre un servizio di ricarica di veicoli elettrici ai conducenti di tali veicoli e fornisce valore consentendo l'accesso a una varietà di punti di ricarica in un'area geografica.

In genere i servizi di un eMSP funzionano in maniera tale che l’utente debba registrarsi e creare un account per poterne usufruire, talvolta però (come imposto da certe leggi locali) gli eMSP possono anche consentire l’accesso agli utenti non registrati.

Insieme a un servizio CPO, un eMSP potrebbe concentrarsi sull'abilitazione dell'accesso alle stazioni di ricarica di una sola società; in alternativa, gli eMSP potrebbero non aver alcuna società di riferimento, o averla ma voler fornire l'accesso anche a stazioni di ricarica di terze parti. In maniera speculare a ciò che è già stato detto per i CPO, ciò è realizzabile tramite l’utilizzo di reti in roaming.

Le due entità, vista la loro somiglianza e l'interconnessione che deve essere presente perché funzionino a dovere, a volte, possono anche essere coincidenti in una stessa società che fa sia da CPO, che da eMSP. Questo però, nonostante sembri uno dei cammini più intuitivi, non sempre viene percorso. In Nord America, ad esempio, EVgo ed Electrify America sono due dei maggiori servizi di eMSP, ma non sono dei CPO: essi assumono altre società per fornire la tecnologia necessaria a far funzionare i loro network di stazioni di ricarica. Questo rende particolarmente importante e degno di attenzione il servizio che crea e gestisce il collegamento tra queste due entità.

OCPI:

OCPI (*Open Charge Point Interface*) è un protocollo open source utilizzato per le connessioni tra operatori di stazioni di ricarica e fornitori di servizi. Esso consente agli utenti finali di utilizzare stazioni di ricarica per veicoli elettrici gestiti da un CPO anche se utilizzano un'app creata da un diverso CPO o eMSP.

In altre parole, questo protocollo facilita il roaming automatizzato per i conducenti di veicoli elettrici su diversi network di ricarica di veicoli elettrici. Questo ruolo è alla base della convenienza e, soprattutto, dell'accessibilità dell'infrastruttura di ricarica per i proprietari di veicoli elettrici, consentendo ai conducenti di caricare il proprio veicolo su diversi network, appartenenti a diverse compagnie e ignorando il complesso scenario di sottili differenze che distinguono aziende di CPO che possiedono anche un eMSP, da aziende che invece possiedono solamente un eMSP senza aver una società di CPO di riferimento e da qualsiasi altra combinazione di possibilità.

Insomma, il ruolo di un protocollo come OCPI, è cruciale nel mercato odierno, sia per permettere all'utente finale di utilizzare in maniera più intuitiva i servizi delle numerose e variegate società che fanno parte del mondo della mobilità elettrica, sia per permettere a quest'ultime una maggior comunicazione e inter-compatibilità.

Capitolo 2

Il protocollo OCPI

2.1 Storia del protocollo OCPI

La prima versione del protocollo OCPI fu originariamente sviluppata nel 2014 da eViolin, una collaborazione di diversi CPO e eMSP olandesi, in cooperazione con ElaadNL, una collaborazione di tutti i maggiori gestori della rete elettrica olandesi.

Dopo un anno, nel 2015, OCPI è stato preso in carico e gestito dalla *Netherlands Knowledge Platform for Public Charging Infrastructure* (NKL), la quale è una collaborazione di organizzazioni commerciali, enti governativi e istituti di ricerca coinvolti nel settore pubblico della ricarica dei veicoli elettrici nei Paesi Bassi.

Nel 2018 è stato istituito un consiglio di amministrazione ad interim più vasto, con 7 soci di diversa estrazione con lo scopo di, figurativamente, "aprire" ancora di più il protocollo, andando a rappresentare anche altri enti del settore interessati allo sviluppo di OCPI. Questo era solo il primo passo di un processo di transizione che ha portato alla nascita della EVRoaming Foundation, una nuova organizzazione indipendente da NKL alla quale sarebbero passate sia la proprietà intellettuale di OCPI, che tutte le autorità e il potere decisionale riguardo lo sviluppo futuro del protocollo.

Attualmente, la gestione del protocollo è, appunto, passata in mano alla EVRoaming Foundation, la quale però in questi anni ha ampliato i suoi interessi e non è più definita solamente dal suo ruolo con OCPI ma supporta anche altre attività e servizi, sempre collegati al mondo della mobilità elettrica. L'EVRoaming Foundation, trattandosi di una fondazione, ha un consiglio di gestione composto da rappresentanti di diverse compagnie, tra cui Freshmile, Chargepoint, Google Maps, EVBOX, Last Mile Solutions e la stessa NKL.

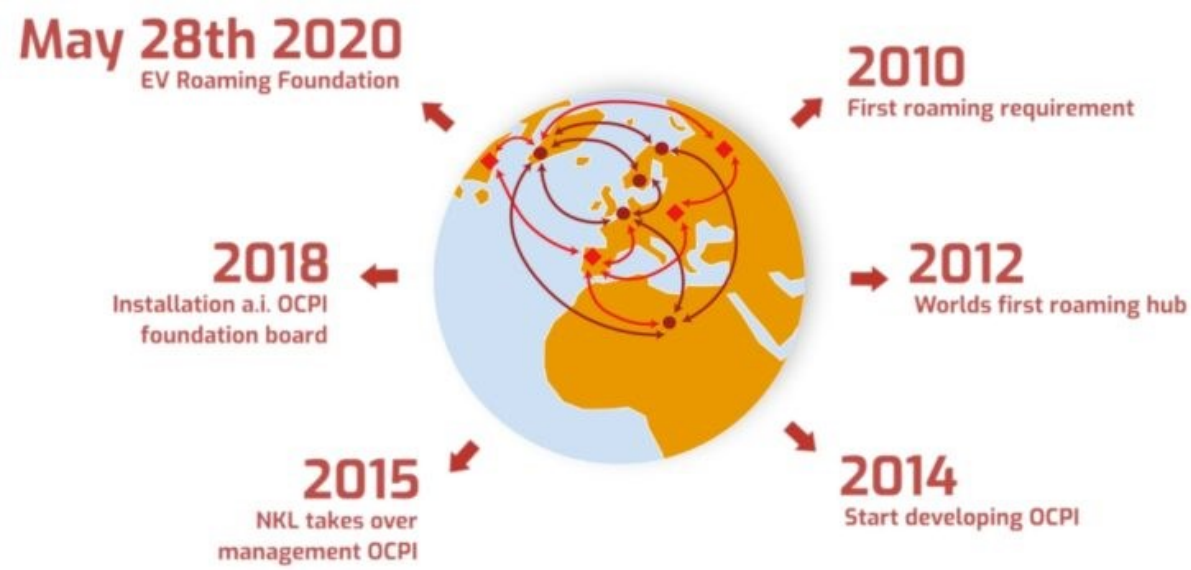


Figura 2 Storia del protocollo OCPI

Per la EVRoaming Foundation, l'obiettivo principale del protocollo Open Charge Point Interface (OCPI) è quello di consentire ai conducenti di veicoli elettrici di ricaricare le proprie auto in qualsiasi stazione sul suolo europeo, indipendentemente dal CPO che gestisce la stazione di ricarica in questione e dall'eMSP che il conducente utilizza. Essa si propone quindi di sviluppare un protocollo gratuito, affidabile e con le potenzialità di essere di portata mondiale, assicurandosi al contempo che questo sia sostenibile e che rimanga accessibile sul lungo termine.

La prima versione ufficiale del protocollo fu rilasciata il 30-12-2015, mentre la versione più recente (v2.2) è stata rilasciata il 04-10-2019.

2.2 Roaming

Come è stato accennato in precedenza, perché un protocollo come OCPI possa funzionare è necessario l'utilizzo di reti in roaming; ebbene il roaming, in ottica più "tecnica" e nel contesto della mobilità elettrica, significa che un conducente di veicoli elettrici sotto contratto con un e-Mobility Service Provider (eMSP) può effettuare una ricarica presso un punto di ricarica gestito da un Charge Point Operator (CPO) con cui il conducente non ha (direttamente) un contratto, ma con il quale l'eMSP ha un contratto, direttamente o tramite un "*roaming hub*".

Perché il roaming sia possibile, poi, deve esserci almeno quanto segue:

- Un accordo contrattuale tra eMSP e CPO, diretto (bilaterale) o indiretto (solitamente tramite un roaming hub)
- Il punto di ricarica deve avere una connessione a Internet;
- un lettore di carte RFID o una funzione per l'attivazione remota;
- dei protocolli di comunicazione interoperabili.

Nell'introduzione è stato fatto presente come la presenza del roaming fosse estremamente importante per l'utente finale, il quale poteva beneficiare di una maggiore convenienza e, soprattutto, accessibilità del sistema di stazioni di ricarica.
La realtà è che questo sistema, per le società che popolano il mercato dei veicoli elettrici, è anche più importante. Per gli eMSP, la logica nello scegliere di implementare il roaming è che possono offrire l'accesso a stazioni di ricarica esterne alle loro e quindi essere più attraenti per i clienti, anche partendo da una posizione monetaria svantaggiata, magari potendosi permettere meno stazioni di ricarica proprietarie di altre aziende più affermate. Per i CPO, invece, la motivazione di questa scelta è semplicemente che, così facendo, ci sono concrete possibilità di aumentare l'utilizzo del proprio network di stazioni di ricarica.

Ci sono anche degli svantaggi, o comunque degli ostacoli, sia per i CPO che per gli eMSP che decidono di implementare il roaming. Questi consistono principalmente nelle risorse necessarie per stabilire e mantenere le connessioni in roaming e, se presenti, alle tariffe da pagare quando ci si connette ad un roaming hub. Inoltre, per alcuni grandi eMSP/CPO, offrire l'accesso esclusivo al loro network è parte centrale del loro modello di business (esempi sono sia Tesla, che alcuni CPO nei paesi nordici e nel Regno Unito) e tali società, attualmente, rappresentano gli attori principali in un'infrastruttura frammentata, piuttosto che un attore solitario in un'infrastruttura interconnessa.

2.2.1 Tipologie di roaming

Esistono principalmente due tipologie di roaming, quella tramite roaming hub e quella peer-to-peer. Mentre la seconda è quella "diretta" che permette alle due entità di entrare in contratto senza alcun tramite, la prima prevede l'esistenza di una terza entità chiamata, appunto, roaming hub che fa da intermediario alla connessione.

Storicamente, le aziende di roaming hub hanno sempre avuto un ruolo centrale nei settori che fanno uso di reti in roaming. Per molti eMSP e CPO, infatti, il vantaggio di connettersi ad un roaming hub è dato dal fatto che questo fornisce un accesso immediato ad un network potenzialmente molto ampio e già sviluppato; questo è cruciale in un mercato come quello della

mobilità elettrica europea che, in questo momento storico, è pieno di piccole realtà. I roaming hub, ovviamente, hanno i loro svantaggi dato che impongono il pagamento di una "tassa" sulla connessione e perché, visto che permettono di connettersi a più entità contemporaneamente, forzano ad attuare la connessione in una maniera specifica.

In alternativa, la connessione peer-to-peer offre più flessibilità nelle modalità usate per connettersi con i partner, dato che questo tipo di cose possono essere decise di volta in volta nelle modalità contrattuali con il partner in questione e possono essere tarate più accuratamente sul servizio; allo stesso tempo però questo lavoro di personalizzazione di ogni accordo rende l'impostazione e la gestione di un network di connessioni peer-to-peer più complessa. Per queste ragioni, normalmente, le connessioni peer-to-peer sono più utili alle aziende più grosse del mercato, le quali hanno le risorse per gestirle. Infine, chiaramente, una connessione peer-to-peer permette di evitare quei costi di "tassazione" che andrebbero altresì pagati ad un roaming hub.

Per semplificare e riassumere, le operazioni peer-to-peer sono favorite tra grandi aziende di CPO/eMSP, le quali hanno un traffico significativo tra di loro, mentre i roaming hub sono una soluzione specialmente utile per piccoli CPO/eMSP, i quali hanno meno risorse da investire, oppure a grandi compagnie di CPO/eMSP che però vogliono connettersi con molte compagnie più piccole.
Questo implica che le connessioni peer-to-peer e l'utilizzo di roaming hub siano realtà complementari e, infatti, ci si aspetta che il futuro riservi un sistema ibrido e non totalmente polarizzato verso una delle due modalità di connessione. Per porre un esempio, tale scenario presenta molte analogie con il campo della telefonia mobile odierno.

2.2.2 Alternative al roaming

In tutto questo esistono anche delle alternative al roaming: i CPO, ad esempio, possono implementare "l'accesso ad hoc", in cui al conducente del veicolo elettrico viene fornito il servizio tramite pagamento diretto; fornire un accesso ad hoc per ogni punto di ricarica (ad es. tramite un terminale per carte di credito), però, può essere costoso. È anche vero che, secondo l'attuale regolamento UE, fornire un accesso ad hoc è obbligatorio per i punti di ricarica pubblici. Al contempo, i metodi di pagamento non sono specificati, né standardizzati, il che ha portato a diverse implementazioni tra i CPO, nullificando il senso di omologazione che una cosa del genere avrebbe potuto portare.

Il roaming può estendere la flessibilità e la portata geografica dei network di stazioni di ricarica; ebbene la stessa identica cosa si può fare anche con gli accessi ad hoc, addirittura senza la necessità di aver alcun contratto e scavalcando direttamente gli eMSP.
Sebbene lo scopo principale del roaming sia ottenibile anche tramite l'accesso ad hoc, il vantaggio che il primo dei due mantiene è che, utilizzando un eMSP, si possono avere anche servizi aggiuntivi come la localizzazione, informazioni aggiuntive sui punti di ricarica e sulle tariffe, assistenza stradale e molti altri (normalmente tramite l'impiego di un'app per telefono).

Si può dire quindi che il roaming e i pagamenti tramite accesso ad hoc siano realtà in competizione, ciascuna con i propri vantaggi e svantaggi; attualmente non è chiaro quale delle due sia più avvantaggiata nel mercato e, probabilmente, nessuna delle due prevarrà sull'altra ma, in futuro, ci sarà bisogno di entrambe.

2.3 Open protocol

Lo sfruttamento delle reti in roaming di cui si è parlato fino a qui è possibile solo grazie all'implementazione di protocolli di comunicazione. Nel mercato sono presenti numerose alternative e OCPI, chiaramente, è una di queste.

Una delle caratteristiche principali che lo distingue dai suoi competitor è il fatto di essere un protocollo "aperto". Questo significa che chiunque può unirsi alla community di OCPI e contribuire al suo sviluppo attraverso la piattaforma online "*Slack*". Il codice sorgente è pubblico e scaricabile senza alcun costo e senza bisogno di alcuna registrazione.
OCPI è pubblicato sotto *Creative Commons Attribution-NoDerivatives 4.0 International Public License*, modello che consente una libera distribuzione (dando, ovviamente, i dovuti crediti) ma proibisce la distribuzione di versioni modificate del protocollo. Per questa ragione OCPI non può essere propriamente definito un protocollo "*open source*", anche se ciò è inevitabile; altrimenti ci sarebbe il rischio che versioni troppo differenti dall'originale e incompatibili tra di loro entrino in circolazione.

Ad ogni modo, sebbene non si possa definire un vero e proprio sviluppo open source, molti dei principi cardine e dei vantaggi di questo tipo di sviluppo sono ancora applicabili.
Lo sviluppo è collaborativo e si basa sulla "*peer review*", ovvero le revisioni condotte dai colleghi e professionisti del settore, e sul lavoro della community. Inoltre, poiché sviluppato da una community e non da una singola azienda o individuo, il software risulta essere una soluzione più flessibile, longeva e trasparente rispetto ai software proprietari.

2.4 Aspetto modulare e funzionalità

Un altro dei grossi vantaggi di OCPI, nello specifico per il suo uso di mercato, è il fatto che si tratti di un protocollo modulare; con questo si intende che tutte le sue funzioni sono divise in "blocchi", i quali possono fare a meno l'uno dell'altro. Un'azienda che decide di adottarlo, perciò, può decidere di includere solamente le funzionalità che le interessano, lasciando da parte il resto, e senza che l'integrità complessiva del protocollo venga compromessa. Le funzionalità aggiuntive poi, nel caso le necessità dell'azienda dovessero cambiare, potranno venir aggiunte in un successivo momento senza che venga richiesto uno sforzo importante, sia dal punto di vista economico che da quello temporale.
Proprio per questo si può definire OCPI come un "one-time investment"; lo sforzo iniziale potrebbe essere significativo per la potenziale difficoltà nel trasferire modelli e processi interni già presenti, omologandoli al linguaggio e agli standard richiesti da OCPI ma, una volta fatto, l'azienda si può aprire per un'integrazione rapida.

OCPI definisce un insieme di moduli che coprono la maggior parte delle casistiche di cui il guidatore potrebbe aver bisogno. Esistono due moduli tecnici, utilizzati per stabilire la connessione tra i due interlocutori (CPO e eMSP) tramite OCPI e che, per questo motivo, sono gli unici fondamentali e obbligatori da implementare per il corretto funzionamento del protocollo: questi sono il modulo "*Credentials*" e il modulo "*Versions*". Come si diceva prima, questi fanno parte del one-time investment necessario perché le società possano adottare OCPI.

Mentre l'importanza del modulo "*Credentials*" è quasi scontata, trattandosi del modulo che abilita la vera e propria comunicazione tra le due entità e senza il quale il protocollo OCPI perderebbe di senso, il motivo dell'importanza dal modulo "*Versions*" è che questo è cruciale per le connessioni peer-to-peer. Non essendo presente alcun intermediario che forza gli aggiornamenti o che blocca l'utilizzo di versioni obsolete, rendere questo modulo obbligatorio è l'unica soluzione per non forzare le società ad aver bisogno di un roaming hub ma poter decidere anche di gestire la connessione in modalità peer-to-peer.

Attualmente, alla versione 2.2, le funzionalità del protocollo sono le seguenti:

- Roaming via hub
- Roaming peer-2-peer
- Roaming with mixed roles
- Authorization
- Reservation

- Provide tariff information
- Billing
- Provide static charge point information (e.g. location)
- Provide real-time charge point status information
- Provide (real-time) session information
- Provide CDR information
- Remote start/stop (for use via mobile app)
- Smart charging support
- Callibration law (eichrecht) support
- Platform monitoring

Alcune di queste corrispondono a dei "moduli", come li si è definiti fino a qui, altre invece sono semplicemente caratteristiche intrinseche del protocollo, come le prime tre della lista. Proprio osservando queste prime tre, inoltre, è importante notare che OCPI fornisce le possibilità di effettuare collegamenti in roaming sia in modalità peer-to-peer, sia tramite l'intermediazione di un roaming hub.

Alcuni esempi di moduli particolarmente importanti che meritano un approfondimento e una piccola descrizione sono "*Locations*", "*Sessions & Commands*" e "*CDRs*".
Il primo dei tre è responsabile della condivisione delle informazioni dei punti di ricarica come l'indirizzo, la geolocalizzazione e altri dati in tempo reale sullo stato attuale come ad esempio se sono fermi per manutenzione o se sono già in uso da parte di un altro utente.
Il secondo, invece, consente all'utente finale di avviare le sessioni di ricarica e di rimanere informato sullo stato di quest'ultime con informazioni quali l'attuale percentuale di carica e il tempo stimato per la conclusione della ricarica, ad esempio.
Per finire, l'ultimo dei tre moduli citati sopra, "*CDRs*", è quello che permette la condivisione e l'invio dal CPO all'eMSP dei dati di resoconto dell'interazione avvenuta, ovvero di tutti quei dati che attestano, alla fine della ricarica, informazioni quali, ad esempio, quanti watt di energia sono stati caricati nell'auto e, soprattutto, qual è il costo della transazione.

Ovviamente, nonostante la flessibilità dell'impianto modulare potrebbe rappresentare un vantaggio importante per molti enti del settore, perché un CPO, ad esempio, possa consentire agli utenti di caricare la propria auto efficacemente (dove qui, chiaramente, si intende farlo attraverso un eMSP dove è OCPI ad abilitare la comunicazione tra i due e non "in assoluto") sarà necessario per esso implementare molti più moduli dei due fondamentali.

Mentre moduli come "*Tokens*" e "*Tariffs*" sono effettivamente opzionali e, in base agli accordi tra le parti, potrebbero anche venir ragionevolmente omessi, altri come "*Sessions & Commands*" e "*CDRs*" sono imprescindibili dalle funzionalità di roaming.

Capitolo 3

Il regolamento europeo GDPR

3.1 Definizione del GDPR

Con il termine GDPR, acronimo di General Data Protection Regulation (Regolamento Generale sulla Protezione dei Dati), ci si riferisce al *"REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)".*
Il documento in questione ha come scopo quello di proteggere i dati personali degli utenti e chiarisce come questi debbano essere trattati, incluse le modalità di raccolta, utilizzo, condivisione e, ovviamente, protezione.

Gli obiettivi del GDPR sono molti: da un lato la normativa vuole rafforzare la protezione dei dati per tutti i cittadini europei e dare loro un maggior controllo su quelli che sono i propri "dati personali"; da un punto di vista più tecnico, invece, l'obiettivo del GDPR è contemporaneamente adeguare la regolamentazione europea alle nuove tecnologie (quella precedente risaliva al 1995) e uniformarla a livello territoriale, creando un quadro normativo comune.

All'interno del documento sono contenuti 99 articoli nei quali viene sancito tutto ciò che fa riferimento alla gestione dei dati personali, in particolar modo, oltre al normale ambito di applicazione, alle varie definizioni, tra cui quella stessa di "dato", e alle sanzioni, viene data particolare enfasi alle responsabilità e alle figure responsabili, alla portabilità e sicurezza dei dati, ai diritti degli interessati.

Presentando in maniera sintetica, tra le numerose normative, alcune delle più significative; per i dati personali viene sancito come questi possano essere trattati solamente se ricorre una delle seguenti sei condizioni, ovvero: (1) consenso, (2) contratto, (3) obbligo legale, (4) salvaguardia degli interessi vitali, (5) interesse pubblico o (6) interesse legittimo. In aggiunta, il GDPR richiede massima trasparenza nei confronti degli utenti i cui dati vengono raccolti in merito a quali vengano raccolti, su quale base giuridica e con quale finalità, per quanto tempo vengono conservati e se sono condivisi con terze parti. Gli interessati hanno inoltre il diritto di richiedere una copia dei dati e di farli cancellare in determinate circostanze.

3.1.1 I dati personali

Una definizione fondamentale data dal GDPR è quella di "dato personale".
Questo perché, in base a quanto una specifica informazione è conforme alle restrizioni date dalla definizione stessa, questa potrà essere definita "dato personale" e sarà quindi considerata sotto la protezione della normativa.
Ebbene, con dato personale si intende: "*qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*".
Alla luce di questa definizione e di altre presenti all'interno del documento si può evincere, in maniera più completa, che sono incluse nella definizione di dati personali anche tutte le informazioni che, se raccolte insieme, possono portare all'identificazione dell'interessato e che, sempre inclusi nella definizione, sono anche i dati crittografati o presentati con l'uso di pseudonimi, finché la crittografia/anonimizzazione è reversibile.

Tali dati possono essere poi distinti in "Provided Data" (forniti consapevolmente e volontariamente), "Observed Data" (raccolti automaticamente ad esempio tramite cookie), "Derived Data" (prodotti da altri dati in modo relativamente semplice e diretto) e "Inferred Data" (prodotti utilizzando un metodo analitico complesso).

3.2 Importanza del GDPR

Il GDPR, alla radice, è una normativa che si basa principalmente sul concetto di privacy e protezione dei dati personali, cosa che il documento rende immediatamente chiaro nel primo punto del Regolamento dove viene sancito che "*la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale*". L'importanza di questi principi è quasi scontata, visti i rischi in cui si può incorrere quando i propri dati personali vengono usati in maniera illecita.

Il GDPR, però, non si limita a stabilire sanzioni e dettare normative sul trattamento sicuro dei dati, esso piuttosto tenta di conferire all'utente un ruolo di protagonista. All'interno, infatti, largo spazio è dato al ruolo dell'utente, il quale deve sempre dare il proprio consenso inequivocabile all'ente che intende trattare i suoi dati. In aggiunta, agli utenti vengono conferiti dei diritti atti a fare in modo che questi ultimi possano mantenere sempre il pieno controllo sui

propri dati. Tra questi diritti spiccano quello di accesso, di rettifica e, soprattutto, quello di cancellazione, che l'utente può far valere nel caso decidesse di revocare il consenso precedentemente dato al trattamento dei propri dati.

La tutela dell'utente, poi, è utilizzata anche come strumento al fine di creare un ambiente sociale in cui questi si sentano di poter dare fiducia alle imprese con i loro dati. Tra gli articoli del GDPR, infatti, viene ad esempio sancito che le organizzazioni e le aziende che entrano in possesso dei dati degli utenti debbano avere sempre dei "Responsabili per la Protezione dei Dati", figure apposite con una conoscenza approfondita della legislazione in materia di protezione dei dati e responsabili del rispetto della stessa. In aggiunta, un'altra manovra in questa direzione è la notifica del data breach, la quale impone al titolare del trattamento dei dati di informare l'autorità di controllo entro 72 ore dal momento in cui viene a conoscenza di una violazione dei dati personali (ovvero un *"data breach"*).

Infine, evidenziando altre misure con gli stessi obiettivi sopracitati e che spingono nella stessa direzione ma cambiando prospettiva e prendendo quella delle aziende, due principi cardine del GDPR sono quello del "*privacy by design*" e dell'"*accountability*". Il primo prevede che, per impostazione predefinita, le imprese dovrebbero trattare solo i dati personali nella misura necessaria e sufficiente per le finalità previste e per il periodo di tempo strettamente necessario ai fini. Il secondo, invece, esprime la necessità, da parte di titolari e responsabili, dell'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento.

In conclusione, in un mondo tecnologicamente sempre più connesso e dove la divulgazione dei dati personali degli utenti per offrire servizi è pratica sempre più comune, per evitare che questi dati vengano usati in maniera indebita, sono necessarie delle tutele. Ebbene, il GDPR tenta di gettare le basi di normativa legale perché gli utenti possano essere resi più consapevoli, più in controllo e, di conseguenza, più sicuri nello sfruttare le possibilità che la rete offre e concedere i propri dati con la fiducia che questi vengano usati in maniera debita.

Citando direttamente dal punto 7 del Regolamento del GDPR: *"Tale evoluzione [parlando dell'evoluzione tecnologica e della globalizzazione] richiede un quadro più solido e coerente in materia di protezione dei dati nell'Unione, affiancato da efficaci misure di attuazione, data l'importanza di creare il clima di fiducia che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno. È opportuno che le persone fisiche abbiano il controllo dei dati*

personali che le riguardano e che la certezza giuridica e operativa sia rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche."

Capitolo 4

Progetto di tesi

4.1 Contestualizzazione del progetto

Sebbene la correlazione tra il protocollo OCPI e il documento di normative europee del GDPR non sia immediatamente visibile, in realtà questa è presente ed è di notevole importanza. OCPI, infatti, come presentato estensivamente nei capitoli precedenti, è un protocollo di comunicazione e, in quanto tale, il suo lavoro è quello di fare da tramite tra i CPO e gli eMSP che lo utilizzano. Questo lo pone nella posizione di gestire gli stessi dati, potenzialmente "personali", che le due entità scambiano tra di loro.
L'importanza del valutare se il protocollo OCPI rispetti le normative imposte dal GDPR, quindi, è iscritta nella necessità di fare in modo che l'intero settore della ricarica di veicoli elettrici rispetti tali regolamentazioni; perché questo succeda ogni singolo "anello della catena" non deve presentare inadempienze, per quanto sia limitato l'utilizzo che questo fa dei dati dell'utente.

4.2 Premesse del progetto

Per il lavoro di analisi e valutazione del rispetto delle normative sulla privacy da me svolto in questo progetto di tesi mi sono basato solamente sullo studio del codice e della documentazione ufficiale rilasciata dalla EVRoaming Foundation della versione 2.1.1 del protocollo OCPI. Non sono stati effettuati test pratici, né simulazioni effettive del protocollo e, in quanto tale, il lavoro è basato su speculazioni, seppur fondate e basate su uno studio preciso e puntuale del materiale a mia disposizione.

Inoltre, nonostante la versione più recente del protocollo OCPI sia la 2.2, questo lavoro è stato fatto basandosi sulla versione 2.1.1. Le motivazioni di questa scelta sono due: per prima cosa l'abbondanza di materiale di studio facilmente reperibile per questa versione, in confronto a quello disponibile per la versione più recente; in secondo luogo, l'aggiornamento all'ultima versione del protocollo da parte delle aziende che lo utilizzano non sempre è tempestiva e, di conseguenza, un lavoro basato su una versione più vecchia non risulta inutile, al contrario può servire ad incentivare le aziende ad aggiornare il protocollo, mettendo in luce difetti o criticità che le versioni più recenti potrebbero aver già provveduto a correggere.

4.3 Applicabilità del GDPR

Innanzitutto, la prima cosa da valutare è se quelli che gestisce OCPI sono considerabili "dati personali". Come spiegato nel capitolo 3 infatti, il GDPR protegge solamente quelle informazioni che vengono definite tali e, se i dati scambiati da OCPI non dovessero rispettare tale definizione, un lavoro di analisi di privacy in prospettiva del GDPR non avrebbe alcun senso. Ricordando, dal capitolo 3, che il GDPR per "dato personale" intende "*qualsiasi informazione riguardante una persona fisica identificata o identificabile*", ciò significa che non importa quali informazioni siano trattate dal protocollo, nel momento in cui l'identità dell'utente non è completamente e irreversibilmente anonimizzata, l'obiettivo di questa verifica è raggiunto e si può ritenere il protocollo OCPI come soggetto alle regolamentazioni del GDPR.

L'oggetto che si vuole prendere in esame per fare questa verifica sono i *Charge Detail Records* (*CDRs*), questo sia perché si tratta di una delle entità più importanti del protocollo, sia per comodità, dato che avrà un ruolo centrale anche più avanti nel corso del lavoro.

Un'importante precisazione è che, nonostante quello dei CDR non si tratti di un modulo dall'implementazione obbligatoria, come già accennato alla fine del capitolo 2, questo è quasi totalmente imprescindibile dalle funzionalità di roaming e del protocollo stesso; per questa ragione tenere in considerazione uno scenario nel quale questo modulo non venga implementato è pressoché inutile.

I CDR contengono il resoconto della transazione avvenuta al momento della ricarica del veicolo elettrico e vengono inviati dal CPO all'eMSP. Riferendosi alla documentazione ufficiale, un CDR è così composto:

Property	Type	Card.	Description
id	CiString(36)	1	Uniquely identifies the CDR within the CPOs platform (and suboperator platforms).
start_date_time	DateTime	1	Start timestamp of the charging session.
stop_date_time	DateTime	1	Stop timestamp of the charging session.
auth_id	string(36)	1	Reference to a token, identified by the auth_id field of the Token.
auth_method	AuthMethod	1	Method used for authentication.
location	Location	1	Location where the charging session took place, including only the relevant EVSE and Connector.
meter_id	string(255)	?	Identification of the Meter inside the Charge Point.
currency	string(3)	1	Currency of the CDR in ISO 4217 Code.
tariffs	Tariff	*	List of relevant tariff elements, see: Tariffs. When relevant, a "Free of Charge" tariff should also be in this list, and point to a defined "Free of Charge" tariff.
charging_periods	ChargingPeriod	+	List of charging periods that make up this charging session. A session consists of 1 or more periods, where each period has a different relevant Tariff.
total_cost	number	1	Total cost (excluding VAT) of this transaction.
total_energy	number	1	Total energy charged, in kWh.
total_time	number	1	total duration of this session (including the duration of charging and not charging), in hours.
total_parking_time	number	?	Total duration during this session that the EV is not being charged (no energy being transfered between EVSE and EV), in hours.
remark	string(255)	?	Optional remark, can be used to provide addition human readable information to the CDR, for example: reason why a transaction was stopped.
last_updated	DateTime	1	Timestamp when this CDR was last updated (or created).

Figura 3 Descrizione dell'oggetto "CDR" nella documentazione ufficiale

Come detto sopra, l'informazione che si vuole estrapolare da questo tipo di entità è se c'è un modo, analizzando le informazioni in essa contenute, di risalire all'identità dell'utente.

Come si può vedere, un CDR contiene svariate informazioni, tra cui il luogo e l'ora dove è avvenuta la ricarica e il costo complessivo di quest'ultima. Queste però, anche se unite insieme, a meno di non aver ulteriori informazioni raccolte da fonti esterne, non sono abbastanza per compromettere l'anonimato dell'utente.

I parametri più interessanti sono invece "*id*" e "*auth_id*", poiché rappresentano dei veri e propri codici identificativi. Il primo dei due però non è molto utile per questa analisi dato che, come c'è scritto nella sua descrizione, identifica in maniera univoca il CDR stesso al CPO e non ha quindi collegamenti con l'utente.

Il secondo invece, "*auth_id*", è più pertinente e si tratta una reference ad un token, un altro tipo di entità che a sua volta contiene queste informazioni:

Property	Type	Card.	Description
uid	string(36)	1	Identification used by CPO system to identify this token. Currently, in most cases, this is the RFID hidden ID as read by the RFID reader.
type	TokenType	1	Type of the token
auth_id	string(36)	1	Uniquely identifies the EV Driver contract token within the eMSPs platform (and suboperator platforms). Recommended to follow the specification for eMA ID from "eMI3 standard version V1.0" (http://emi3group.com/documents-links/) "Part 2: business objects."
visual_number	string(64)	?	Visual readable number/identification as printed on the Token (RFID card), might be equal to the auth_id.
issuer	string(64)	1	Issuing company, most of the times the name of the company printed on the token (RFID card), not necessarily the eMSP.
valid	boolean	1	Is this Token valid
whitelist	WhitelistType	1	Indicates what type of white-listing is allowed.
language	string(2)	?	Language Code ISO 639-1. This optional field indicates the Token owner's preferred interface language. If the language is not provided or not supported then the CPO is free to choose its own language.
last_updated	DateTime	1	Timestamp when this Token was last updated (or created).

Figura 4 Descrizione dell'oggetto "Token" nella documentazione ufficiale

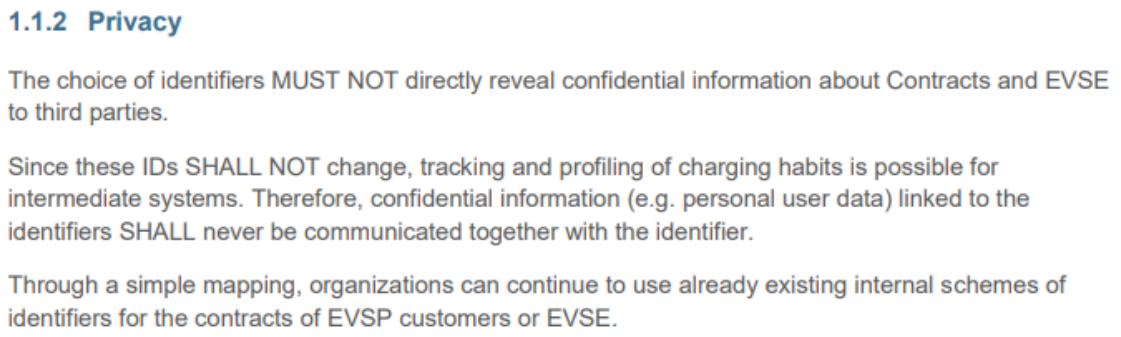
Come è possibile intuire guardando la struttura e i parametri che compongono quest'entità, il token è un elemento centrale di un altro modulo di OCPI (chiamato, appunto, "Token module"). Anche questo modulo non è obbligatorio ma, dato che è impossibile implementare il modulo CDR senza il modulo Token, il discorso fatto precedentemente è valido anche in questa occasione.

Lo scopo dell'entità Token è quello di identificare univocamente sia per il CPO che per l'eMSP una specifica transazione e per farlo si avvale di diversi parametri, tra i più significativi sono "*uid*", *auth_id*" e "*visual_number*". Come vedremo, però, "*uid*" e "*visual_number*" sono assimilabili allo stesso discorso.

Il primo dei due, infatti, è un parametro che contiene una stringa, la quale serve per identificare e legare la transazione (e quindi il token stesso) al CPO. Di per sé, concettualmente, un identificativo del genere non sarebbe legato all'utente, se non fosse che, come si può leggere dalla descrizione del parametro, il codice utilizzato è, nella maggior parte dei casi, l'hidden ID di una RFID card. Ebbene, visto che il parametro "*visual_number*" ha al suo interno il codice non-hidden della RFID card, questo spiega il perché si possa accorpare entrambi ad un unico discorso prendendo in esame le RFID card.

In questa situazione, con RFID card, solitamente si intendono delle "carte fedeltà", le quali possono essere adottate sia dalle aziende di CPO, che dalle aziende di eMSP per permettere all'utente di autenticarsi e di effettuare pagamenti. Indagare nel dettaglio quanto questo tipo di tecnologia renda anonimo l'utente, però, è fuori dagli obiettivi di questo progetto di tesi. Il motivo è dato dal fatto che si tratta di un sistema troppo variabile e altamente stratificato. Oltre alla variabilità data dalle numerose aziende di CPO e eMSP che utilizzano sistemi, procedure e linee guida diverse, anche il solo concetto di "carta fedeltà" potrebbe essere una rappresentazione inaccurata per molte di queste realtà. Infine, trattandosi di un sistema legato sia all'autenticazione che al sistema di pagamento, questo a sua volta è legato a realtà bancarie e ciò crea un nuovo percorso che dovrebbe essere analizzato per capire se, attraverso di esso, sia possibile risalire all'identità dell'utente. L'argomento, perciò, è troppo ampio per poter essere preso in analisi da questo progetto di tesi.

Il parametro "*auth_id*", invece, come si può leggere nella sua descrizione, contiene al suo interno una stringa che serve ai sistemi di eMSP per identificare univocamente l'utente. In questo caso è abbastanza chiaro come questo parametro, se non totalmente anonimo, possa permettere di risalire all'identità dell'utente. Ebbene, il problema che si riscontra è la mancanza di vincoli imposti dal protocollo sulla scelta di questo identificatore. All'interno della descrizione del parametro, infatti, è presente un rimando a degli standard da seguire per la scelta dell'identificatore ma si tratta solamente di linee guida raccomandate e non imposte. Inoltre, anche cercando all'interno di questo link, le uniche indicazioni in materia di privacy sono le seguenti:



1.1.2 Privacy

The choice of identifiers MUST NOT directly reveal confidential information about Contracts and EVSE to third parties.

Since these IDs SHALL NOT change, tracking and profiling of charging habits is possible for intermediate systems. Therefore, confidential information (e.g. personal user data) linked to the identifiers SHALL never be communicated together with the identifier.

Through a simple mapping, organizations can continue to use already existing internal schemes of identifiers for the contracts of EVSP customers or EVSE.

Figura 5 Indicazioni di privacy dell'eMobility ICT Interoperability Innovation Group

Come si può vedere, le raccomandazioni specificano effettivamente che la scelta dell'identificativo non dovrebbe rivelare informazioni confidenziali, né dovrebbe in alcun modo essere legato all'utente e alla sua identità. D'altro canto, queste rimangono delle semplici raccomandazioni e, perciò, non è possibile assumere con certezza che vengano rispettate. Il

fatto che il protocollo non imponga degli standard rigidi per la scelta dell'identificativo lascia spazio alla possibilità che questo non sia completamente anonimo.

Inoltre, nonostante prendendo in considerazione i parametri "*uid*" e "*visual_number*" ci si sia concentrati sull'aspetto del legame con le RFID card, lo stesso tipo di discorso è valido anche per quegli identificativi. Non esistendo dei vincoli e delle imposizioni da parte del protocollo OCPI sul tipo di identificativi che devono essere usati e su dei rigidi criteri di anonimato, anche in quel caso c'è la concreta possibilità che il protocollo venga implementato con dei parametri che non tengono conto della privacy dell'utente o che utilizzano identificativi arbitrari e non completamente anonimi.

In entrambi i casi, perciò, si può concludere dicendo che il protocollo non è sicuro abbia al suo interno degli identificativi che permettono di risalire all'identità dell'utente e che quindi non siano completamente anonimi ma, al contempo, non è nemmeno possibile escludere completamente questa possibilità dato che la documentazione di OCPI non pone restrizioni forti alla scelta degli identificativi da utilizzare ma solamente linee guida; ciò rende un lavoro di analisi di privacy del protocollo OCPI in prospettiva del GDPR sensato e necessario.

4.4 Analisi di privacy

Il principio dal quale sono voluto partire è che uno dei requisiti applicativi più importanti per il rispetto del GDPR è che gli unici dati a venir processati siano quelli strettamente necessari per lo svolgimento di un qualunque compito specifico e che questi vengano manipolati solo da quei soggetti che hanno assolutamente bisogno di farlo. In quest'ultima definizione, con i verbi "processare" e "manipolare", ci si riferisce a delle azioni che si possono suddividere, a grandi linee, in tre tipologie: trasmissione, archiviazione ed eliminazione. Per valutare il rispetto delle normative del GDPR da parte del protocollo OCPI, quindi, ho suddiviso l'analisi in tre sottosezioni, ognuna corrispondente ad uno di questi tre aspetti chiave.

Nello specifico, in questo progetto di tesi, ho voluto dare particolare attenzione ed approfondimento alla componente di "trasmissione"; questo sia perché la natura del protocollo in sé è incentrata sulla comunicazione e quindi sulla trasmissione dei dati, sia per una scelta personale. Alcune considerazioni sono state fatte anche rispetto alle altre due tipologie ma mancano di approfondimento.

4.4.1 Trasmissione dei dati

Come scritto in maniera più generica nella sezione precedente, la cosa importante da verificare in questo specifica casistica di "trasmissione" è se i dati personali dell'utente che passano attraverso il protocollo OCPI e che questo invia, siano effettivamente mandati soltanto alle entità che è strettamente necessario li abbiano. Il problema di un controllo di questo tipo è che molto poco dipende dal protocollo OCPI stesso.

Esso, infatti, si tratta di un protocollo "di mezzo" usato dai CPO e dagli eMSP per comunicare, per questa ragione quali dati vengono mandati e a chi questi siano indirizzati non è competenza di OCPI, il quale si limita a consentire la comunicazione tra i due. D'altro canto, esistono una serie di misure che il protocollo OCPI potrebbe implementare per vincolare le possibilità di CPO e eMSP ed impedire così comportamenti potenzialmente illeciti, o anche semplici errori. Questo tipo di misure però non ci sono e, al contrario, diversi pezzi della documentazione del protocollo OCPI mostrano chiaramente che questo tipo di infrazioni sono state identificate come possibili ma, nonostante ciò, non sono state adottate contromisure di sicurezza più elevate per contrastarne l'eventualità.

La documentazione, infatti, scrive:

- *"CDRs are created by the CPO. They probably only will be sent to the eMSP that will be paying the bill of a charging session."*
- [Dopo aver detto che il CPO, dopo aver creato il CDR della transazione, deve inviarlo all'eMSP]
  "A CPO is not required to send ALL CDRs to ALL eMSPs, it is allowed to only send CDRs to the eMSP that a CDR is relevant to."
- [Dopo aver detto che l'eMSP può fare una GET sui CDR del CPO, i quali sono tenuti tutti in una cache]
  "A CPO is not required to return all known CDRs, the CPO is allowed to return only the CDRs that are relevant for the requesting eMSP."

Anche in questo caso l'oggetto preso a riferimento è il CDR, il cui scopo e la cui composizione sono già state spiegate precedentemente. Come si può leggere, nella prima delle tre frasi prese ad esempio dalla documentazione, si dice che questo oggetto, contente informazioni che abbiamo stabilito ci siano possibilità concrete che possano permettere di risalire all'identità dell'utente, *probabilmente* verrà spedito solamente all'eMSP che ne necessita per fare in modo che la transazione avvenga correttamente. Come questa, anche le restanti due frasi sono

problematiche per lo stesso identico motivo, ovvero delle minuzie di linguaggio che non negano completamente la possibilità che questi dati vengano trasmessi anche ad entità che non dovrebbero riceverli, lasciando spazio così a pratiche che violerebbero il GDPR. Ad esempio, la prima parte della terza frase, per come è stata formulata, implica che sarebbe accettabile per un CPO, ad un eMSP che richiede un CDR, mandargli tutti quelli disponibili, compresi quelli di altri utenti non rilevanti all'eMSP stesso.

Come nella verifica precedente sull'applicabilità del GDPR e l'anonimato dei dati, perciò, non è stato riscontrato che OCPI permetta attivamente violazioni del GDPR, poiché il suo ruolo nella comunicazione non è di protagonista e l'invio dei dati parte dai comandi lanciati dai CPO o dagli eMSP. Allo stesso modo di prima, però, non si può nemmeno dire che il protocollo OCPI sia al sicuro da potenziali infrazioni dato che, all'interno della documentazione (e quindi, si suppone, anche del codice), non sono presenti vincoli forti che impediscano pratiche che porterebbero ad una violazione delle norme del GDPR.
In questa occasione, inoltre, la gravità del problema è maggiore, sia perché questa verifica aveva come obiettivo quello di mettere in luce come il protocollo possa presentare al suo interno delle violazioni del GDPR e non la semplice applicabilità o non applicabilità di quest'ultimo, sia perché è evidente dal modo in cui sono state formulate le suddette frasi riportate dalla documentazione che questo tipo di problematiche sono state identificate ma volutamente ignorate in fase di sviluppo.

4.4.1.1 Rischi e conseguenze

Uno scenario ipotetico che permette di capire la gravità e i rischi che derivano da possibili infrazioni del GDPR di questo tipo lo si può inquadrare facilmente analizzando nuovamente nel dettaglio la composizione di un CDR. Quest'ultimo, infatti, oltre ad avere un codice identificativo che abbiamo stabilito abbia concrete possibilità di poter essere ricondotto all'utente, contiene al suo interno parametri quali il luogo (con relative coordinate geografiche) dove è stata effettuata la ricarica del veicolo elettrico, il tempo impiegato, il quantitativo di energia che è stata caricata e il suo costo complessivo.

Queste informazioni, oltre ad essere chiaramente personali, potrebbero anche portare ad un rischio per la sicurezza dell'utente e ciò incrementa la gravità delle conseguenze, le quali non sono più solamente legate ad una compromissione di privacy. La mancanza di misure di sicurezza e di certezze che i dati di un CDR finiscano solamente ai CPO o agli eMSP che ne necessitano, infatti, potrebbe permettere a dei malintenzionati con intenti criminali di farsi riceventi di questi dati. Una volta in loro possesso, una lista dei CDR di uno specifico utente

potrebbe permettere di profilare il suo veicolo, i luoghi dove più frequentemente si reca per ricaricarlo, per quanto tempo si assenta quando lo fa e, potenzialmente, potrebbe anche essere possibile attraverso queste informazioni ricostruire parte delle abitudini dell'utente.

Per questa ragione, è di fondamentale importanza che, come si diceva nel paragrafo di contestualizzazione del progetto di tesi, anche un protocollo come OCPI, il quale ha un ruolo, seppur fondamentale, di piccola entità nel settore della ricarica dei veicoli elettrici, rispetti le normative europee del GDPR. Queste, infatti, sebbene abbiano come obiettivo principale quello di proteggere la privacy dell'utente, spingono anche ad implementare delle misure di sicurezza aggiuntive e, inoltre, attraverso la preservazione della privacy, contemporaneamente impediscono l'esistenza di pratiche criminali come quella appena esposta, basate sul non completo anonimato dell'utente.

4.4.2 Archiviazione ed eliminazione dei dati

Per finire, da valutare sono rimasti gli ambiti di archiviazione ed eliminazione dei dati. Come già anticipato precedentemente, ho deciso di non approfondire l'analisi di questi ambiti allo stesso modo di come ho fatto per quello di trasmissione; nonostante ciò, ad un controllo più superficiale, anche su questi versanti ho individuato quelle che potrebbero essere delle gravi problematiche.

Innanzitutto, è fondamentale inquadrare il punto di partenza della mia ridotta analisi, ovvero il fatto che, riferendosi a questi ambiti, perché le normative del GDPR vengano rispettate, una delle cose di cui è necessario assicurarsi è che nel momento in cui i dati personali di un utente non sono più necessari, questi vengano prontamente eliminati.

Per capire se questo requisito del GDPR viene regolarmente applicato è necessario, per prima cosa, comprendere come funziona il sistema di archiviazione del protocollo OCPI, quali dati vengono conservati, in che formato e per quanto tempo. Queste informazioni, però, non sono chiare nella documentazione e, in essa, non vi è alcun riferimento dettagliato al riguardo se non il fatto che OCPI adopera una cache nella quale, tra le altre cose, vengono perlomeno sicuramente conservati i CDR. Sebbene non sia chiaro se questa sia l'unico sistema di archiviazione del protocollo o ne esistano altri, né quale siano le specifiche regole che questa cache segue, come è già stato ampiamente discusso, i CDR ricadono in ciò che si può definire "dati personali" per l'utente e, di conseguenza, il fatto che questi vengano certamente archiviati, anche solo almeno per un periodo, all'interno di una cache, impone al protocollo OCPI di trattarli prestando attenzione alle normative del GDPR che regolano i suddetti dati.

Un CDR, infatti, tra le altre cose, contiene il codice identificativo dell'utente, il luogo dove è stata effettuata la ricarica, il giorno e l'ora, il quantitativo di energia caricata e il costo totale della transazione. Dopo che la transazione è terminata e l'utente ha ricevuto l'addebito però, informazioni come il luogo o il giorno e l'ora, ad esempio, potrebbero non essere più rilevanti da mantenere e, in tal caso, dovrebbero venir rimosse.

Questa cosa però, allo stato attuale, è impossibile che avvenga poiché OCPI, per assicurarsi dell'autenticità delle transazioni e del fatto che queste non siano state compromesse in alcun modo, prevede un meccanismo di "firma semplice" sull'intero CDR. Senza entrare nel merito del meccanismo, questo comporta che un CDR deve essere immutabile e la rimozione di informazioni, anche solo parziali, come ad esempio il giorno e l'ora, andrebbe ad invalidare la firma e, conseguentemente, la transazione che il CDR rappresenta.

Un meccanismo di firma così implementato, su tutto il CDR, inoltre, è in contrasto anche con un altro requisito del GDPR utilizzato precedentemente, ovvero il fatto che i dati debbano venir elaborati solamente da quelle parti che hanno assoluto bisogno di farlo. I messaggi ricevuti ed inoltrati dai CPO, infatti, spesso portano parti di informazioni destinate solamente al CPO, le quali non c'è motivo per il quale dovrebbero essere inoltrate anche all'eMSP. Ad esempio, si potrebbe dire che, ragionevolmente, un eMSP non ha mai bisogno di ricevere in un CDR le informazioni sulla posizione dell'utente. Con il meccanismo di firma attuale però, come già detto, non è possibile eliminare selettivamente una porzione del CDR senza invalidare l'intera firma.

Per finire, un ultimo possibile problema legato a questo tipo di meccanismo è che, oltre all'impossibilità di venir modificati, i CDR non possono nemmeno venir cancellati. Questo viola un ulteriore dei requisiti del GDPR ovvero il fatto che l'utente dovrebbe poter richiedere in qualsiasi momento l'eliminazione di tutti i propri dati personali ma, per come è strutturato il protocollo, questo porterebbe all'invalidazione di tutti i CDR e, quindi, di tutte le transazioni compiute dall'utente fino a quel momento.

Come è stato spiegato perciò, per quanto senza un approfondimento più preciso del sistema di archiviazione non sia possibile trarre delle conclusioni certe al riguardo, questo meccanismo di sicurezza che OCPI utilizza nel gestire i CDR pare sia fonte di numerose possibili violazioni dei requisiti imposti dalle normative del GDPR. Inoltre, un ulteriore conferma di queste supposizioni è data dagli sviluppatori stessi, i quali, all'interno della documentazione, riportano

che: *"CDRs can not yet be updated or removed. This might be added in a future version of OCPI"*.

4.5 Conclusione

In conclusione, da questa analisi si può evincere che, nonostante i limiti di questo lavoro dati dalla mancanza di test pratici, e quindi di conferme concrete a supportare le ipotesi e lo studio della documentazione e di autorevoli articoli al riguardo, il protocollo OCPI presenta delle chiare inadempienze delle normative europee sulla privacy. Diversi requisiti applicativi, infatti, non sono rispettati sia in ambito di "trasmissione" dei dati, sia in ambito di "archiviazione ed eliminazione" e questo rappresenta un problema grave non solo in materia di privacy ma, come brevemente esposto nel paragrafo di "Rischi e conseguenze", anche di sicurezza per l'utente.

In luce di ciò, è importante che lo sviluppo del protocollo OCPI proceda in maniera da adeguarsi agli standard richiesti dal GDPR e che le aziende che ancora utilizzano la versione 2.1.1 del protocollo aggiornino i propri sistemi ad una più recente, la quale potrebbe aver già corretto alcune delle mancanze. Nonostante queste non siano state prese in considerazione da questa analisi, infatti, osservandone rapidamente la documentazione senza compiere nessuno studio più approfondito, è possibile notare che nell'ultima versione, la 2.2, il meccanismo che impediva la modifica e l'eliminazione dei CDR è stato cambiato ed è quindi possibile che la problematica da me individuata che affliggeva l'ambito di "archiviazione ed eliminazione" sia stata già presa in carico dagli sviluppatori e conseguentemente risolta. In ogni caso, è auspicabile che le versioni future siano più attente sul fronte della sicurezza e della privacy.

Una mancanza di impegno nei confronti di queste tematiche, infatti, specialmente in un settore come quello della mobilità elettrica, potrebbe portare a gravi danni. Questo perché tratti caratteristici di un settore in crescita sono la grande espansione e diffusione al pubblico, l'ingresso di numerose compagnie nel settore, dalle più piccole che nascono proprio sulla base di nuove esigenze del settore, alle più grandi che tentano di ricavarsi un posto in un nuovo business; tutto ciò porta ad uno sviluppo repentino e altamente multiforme, il quale però, ad un certo punto, tenderà a stabilizzarsi, creando quell'infrastruttura di aziende e compagnie che fungerà da base a tutta l'evoluzione futura del settore. Ebbene, se in questa fase le problematiche di sicurezza e privacy vengono accantonate o addirittura ignorate, ciò che si verrà a creare alla fine sarà un'infrastruttura fallace ed estremamente vulnerabile, la quale porterà l'intero settore a condividere inevitabilmente le stesse caratteristiche. Inoltre, aspettare l'assestarsi di questa turbolenta crescita per dedicare il proprio impegno su questo fronte è

chiaramente un errore poiché, una volta che l'infrastruttura si sarà creata, sarà estremamente proibitivo apporne le modifiche, magari anche di significativa entità, che saranno necessarie per renderla conforme agli standard di sicurezza e privacy. L'unica soluzione, in definitiva, è dedicare ora la giusta attenzione ad uno degli ambiti più cruciali per lo sviluppo e l'espansione di un settore, ovvero quello di sicurezza.

Bibliografia e Sitografia

About Us. EVRoaming Foundation. (2018). https://evroaming.org/about-us/

Accountability (responsabilizzazione). Approccio basato sul rischio e misure di accountability (responsabilizzazione) di titolari e responsabili. Garante per la protezione dei dati personali. https://www.garanteprivacy.it/regolamentoue/approccio-basato-sul-rischio-e-misure-di-accountability-responsabilizzazione-di-titolari-e-responsabili

BARBERIO, R. (2018). *GDPR, L'importanza del fattore umano e organizzativo*. Privacy Italia. https://www.privacyitalia.eu/gdpr-limportanza-del-fattore-umano-e-organizzativo/9118/

BASMADJIAN, R. (2021). *Communication Vulnerabilities in Electric Mobility HCP System: A Semi-Quantitative Analysis.*

BOTTINI, S. (2019). *Infrastrutture e veicoli connessi: il futuro del settore automative*. Il blog di CercaOfficina.it. https://www.cercaofficina.it/blog/infrastrutture-e-veicoli-connessi-il-futuro-del-settore-automotive/

BOTTINI, S. (2019). *La sicurezza informatica in un automotive sempre più connesso*. Il blog di CercaOfficina.it. https://www.cercaofficina.it/blog/officine-e-sicurezza-informatica-in-un-automotive-sempre-piu-connesso/

Che cosa significa open source?. Red Hat. (2019). https://www.redhat.com/it/topics/open-source/what-is-open-source

EMI^3. (2015). *V 1.0 Electric Vehicle ICT Interface Specifications. Part 2: Business Objects.*

EMSP and CPO: the two sides of EV charging network operators. Virta. (2022). https://www.virta.global/blog/emsp-cpo-ev-charging-roles-responsibilities

EVROAMING FOUNDATION. (2017). *OCPI 2.1.1 – Open Charge Point Interface 2.1.1, document version: 2.1.1.*

FERREIRA, J. C. & FERREIRA DA SILVA, C. & MARTINS J. P. (2021). *Roaming Service for Electric Vehicle Charging Using Blockchain-Based Digital Identity. Energies.* 2021; 14(6):1686

FERWERDA, R. & BAYINGS, M. & VAN DER KAM, M. & BEKKERS, R. (2018). *Advancing E-Roaming in Europe: Towards a Single "Language" for the European Charging Infrastructure*. *World Electric Vehicle Journal.* 9(4):50.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI. (2018). *Regolamento generale sulla protezione dei dati – Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016. Arricchito con riferimenti ai Considerando. Aggiornato alle rettifiche pubblicate sulla Gazzetta Ufficiale dell'Unione europea 127 del 23 maggio 2018.*

GDPR e DATA PROTECTION – Tutto sulla protezione dei dati personali prima e dopo il Regolamento europeo. https://blog.osservatori.net/it_it/gdpr-protezione-dati-personali

GIREVE (2021). OCPI Protocol IOP – OCPI Interface - Implementation Guide V1.1.6.

Guida completa al GDPR: tutto quello che c'è da sapere per essere in regola. Iubenda. https://www.iubenda.com/it/help/5424-guida-gdpr#applicazione

GUERRASIO, G. (2018). *GDPR: cos'è e per quali dati si applica?* Viralbeat – Digital Agency. https://www.viralbeat.com/blog/gdpr-approfondimento-privacy/

KLAPWIJK, P. & DRIESSEN, L. (2017). EV related Protocol Study

MAASE, S. & VAN DEN HOED, R. (2019). *EV Charging Data Management, five issues to solve*. 32nd Electric Vehicle Symposium (EVS32). Lyon, France, May 19 – 22, 2019.

MAJCHER, P. (2020). *OICP and OCPI protocols – open standards for CPOs and eMSPs*. Solidstudio https://solidstudio.io/blog/oicp-ocpi-protocols

MAJCHER, P. (2021). *CPO vs EMSP – what's the difference*. Solidstudio. https://solidstudio.io/blog/emobility-fundamentals-cpo-vs-emsp

OCPI Basics. EVRoaming Foundation. (2018) https://evroaming.org/ocpi-background/

Open Protocols. Green Flux. (2021) https://www.greenflux.com/spotlights/open-protocols/

SAETTA, B. (2018). *Privacy by design e by default*. Protazione dati personali. https://protezionedatipersonali.it/privacy-by-design-e-by-default

VALENTINI, A. (2022). *Privacy, guida sintetica per le aziende: ecco cosa fare*. InformazioneFiscale. https://www.informazionefiscale.it/privacy-guida-gdpr-aziende-cosa-fare

VAN AUBEL, P. & POLL, E. (2020). *Security of EV-Charging Protocols.*

VAN DER KAM, M. & BEKKERS, R. (2020). *Comparative analysis of standardized protocols for EV roaming.* Report D6.1 for the evRoaming4EU project.

VAN DER KAM, M. & BEKKERS, R. (2020). *Achieving interoperability for EV roaming: Pathways to harmonization*. Report D6.2 for the evRoaming4EU project.

VAN DER KAM, M. & BEKKERS, R. (2020). *Design principles for an 'ideal' EV roaming protocol.* Report D6.3 for the evRoaming4EU project.

VAN DER KAM, M. & BEKKERS, R. (2020). *Developing roaming protocols for EV charging: Insights for the field*. Proceedings of 8th Transport Research Arena TRA 2020, April 27-30, 2020, Helsinki, Finland

What is OCPI?. Chargelab. https://www.chargelab.co/industry-advocacy/ocpi