

POLITECNICO DI TORINO

Corso di Laurea Magistrale in Ingegneria Gestionale



MACHINE DATA E AUTOMOBILI CONNESSE: TECNOLOGIE, NUOVE NORMATIVE E PRIVACY

Relatore:

Prof. Carlo Cambini

Candidato:

Riccardo Cafarelli

Anno Accademico 2024-2025

INDICE

Introduzione	4
Capitolo 1-Il concetto di “veicolo connesso”	5
1.1 Panoramica generale	5
1.2 Storia	8
1.3 Mercato	11
Capitolo 2-Stakeholders e dati	14
2.1 Carmaker	14
2.2 Assicurazioni	19
2.3 Gestori delle flotte	23
2.4 Mercato europeo dei Machine Data	24
2.5 Mercato europeo dei dati	28
2.6 Data Marketplace	31
2.7 Valorizzazione dei dati	34
Capitolo 3-Normative	38
3.1 Inizi e contesto	38
3.2 GDPR	41
3.3 Data Act	44
3.4 Data Governance Act	50
Capitolo 4-Cybersecurity e Privacy	54
Capitolo 5-Guida autonoma	70
Capitolo 6-Prospettive future	78
Conclusioni	85
Bibliografia e sitografia	87
Ringraziamenti	94

Introduzione

La crescente presenza di utenti, dispositivi connessi e servizi digitali aumenta esponenzialmente il volume di dati prodotti giorno per giorno e sta diventando un elemento cruciale per l'innovazione e la sicurezza pubblica. Nonostante l'enorme potenziale, secondo la commissione europea circa l'80% dei dati industriali non viene utilizzato. Per stimolare la creazione di un mercato unico dei dati e assumere un ruolo di primo piano nella data economy, la commissione europea ha definito una strategia che prevede l'introduzione di alcune normative che regolino l'utilizzo dei dati. Tra queste troviamo il Data Act che regola l'accesso, la portabilità, l'utilizzo e la condivisione dei dati mentre il Data Governance Act si concentra sui fornitori di servizi di intermediazione, l'altruismo, il riutilizzo di dati detenuti da enti pubblici e il flusso di quelli internazionali.

Quando si parla di grandi quantità di dati generati, entrano in gioco le auto moderne che rappresentano dei veri e propri sistemi di raccolta dati su ruote; infatti, un termine utilizzato recentemente è quello di "veicolo connesso" oppure "smart car". Le nuove tecnologie e i vari tipi di sensori permettono di accumulare enormi quantità di dati in tempo reale. Da un lato questo progresso tecnologico ha migliorato l'esperienza di guida, permesso di ottenere sconti in base allo stile di guida, ottimizzato la gestione delle flotte e incrementato la sicurezza dei veicoli, ma dall'altro lato emerge un forte problema di privacy e cybersecurity visto che tali dati vengono venduti o condivisi con diversi soggetti portando al rischio di violazioni come quelli subiti da Toyota, Volkswagen e Audi.

Guardando al futuro, i veicoli a guida autonoma saranno sicuramente i protagonisti, con diverse case automobilistiche che stanno effettuando investimenti e test a riguardo. Questo significa che i veicoli avranno un numero sempre crescente di strumenti tecnologici per la guida; infatti, in base ad un'analisi condotta da McKinsey & Company, i sistemi avanzati di assistenza alla guida (ADAS) e quelli di guida autonoma (AD) potrebbero determinare un introito economico tra i 300 e i 400 miliardi di dollari nel mercato delle auto entro il 2035. Tutto questo ovviamente si riflette in un continuo incremento di dati prodotti dai veicoli nei prossimi anni.

Capitolo 1-Il concetto di “veicolo connesso”

1.1 Panoramica generale

Negli ultimi anni sono diversi i settori che sono stati sottoposti al processo di digitalizzazione e tra questi è presente anche il settore dell'automotive, nel quale un nuovo modo di concepire l'auto, ha portato alla diffusione del termine “veicolo connesso”.

Le auto connesse sono dei veicoli dotati di sistemi GPS, sensori, telecamere, connessione internet e tecnologie innovative che permettono di trasmettere e condividere informazioni con infrastrutture, veicoli, dispositivi e pedoni, realizzando una rete di mobilità intelligente.

Queste autovetture moderne influenzano diversi contesti tra cui

- Sicurezza stradale
 - Sono presenti diverse tecnologie software e hardware capaci di individuare pericoli provenienti da fattori esterni o interni al veicolo come quelli per individuare segnali di stanchezza del conducente. In aggiunta, permettono di scambiare informazioni con altre auto e di richiedere assistenza con il dispositivo eCall in caso di incidente.
- Informazione e intrattenimento
 - Tramite assistente vocale e display touch si può accedere a servizi di infotainment che permettono sia di ottenere dati in tempo reale come nel caso di previsioni metereologiche, condizioni del traffico e navigazione GPS ma anche servizi di svago come la riproduzione di musica.
- Servizi di assistenza
 - Attraverso i display della propria auto si ricevono dati riguardo a manutenzione e stato dei componenti del veicolo.
- Assicurazione basata sull'utilizzo
 - I dati raccolti dall'auto mostrano lo stile di guida del guidatore consentendo così di creare polizze su misura e diversi premi assicurativi sulla base del comportamento del conducente.
- Gestione della flotta
 - Consiste nel monitoraggio di un parco veicoli di un'azienda per ottimizzare costi, consumi e manutenzione. Questo ambito può includere i noleggi e il leasing.
- Guida autonoma
 - Sia quella parziale che totale è supportata da sistemi software e hardware come gli ADAS e la rete V2X.

La protagonista è la tecnologia V2X (Vehicle to Everything) che sfrutta la connettività cellulare e la tecnologia wireless per far in modo che i veicoli possano condividere dati tra di loro e con l'ambiente esterno. La V2X comprende diversi tipi di tecnologie di comunicazione: V2N, V2V, V2I, V2P, V2D, V2C, V2G.

Tramite la tecnologia V2N (Vehicle to Network) che sfrutta le reti cellulari 5G ed LTE e i sistemi di comunicazione a corto raggio (DSCR), i veicoli possono comunicare con pedoni (V2P), cloud (V2C), infrastrutture (V2I) ed altri veicoli (V2V).

La V2V (Vehicle to Vehicle) avviene tramite un trasmettitore DSCR (dedicated short range communication) per la comunicazione wireless a corto raggio, che permette la trasmissione di dati sullo stato del veicolo come direzione, posizione e velocità. Alcuni incidenti tra veicoli si possono evitare sfruttando lo scambio di dati anticipato su possibili pericoli lungo il percorso. Un'altra opzione per la V2V è la Vehicular Ad hoc Network (VANET), ovvero una rete tra veicoli, i quali sono dei nodi in grado di trasmettere e ricevere dati senza il supporto di un'infrastruttura. La comunicazione V2V segna un notevole progresso negli ADAS, inclusa l'identificazione di angoli ciechi. Non solo, il modello tradizionale in cui i veicoli connessi si basano in maniera esclusiva ai dati forniti dai loro sensori, manifesta dei vincoli specialmente per quanto riguarda l'acquisizione di informazioni cruciali oltre il raggio d'azione dei sensori. Si possono verificare situazioni pericolose se ad esempio, un'auto che sta per cambiare corsia non riesce ad individuare un'altra auto ad elevata velocità che sta occupando quella corsia perché si trova al di fuori del campo visivo del sensore. In aggiunta, alcuni ADAS essenziali come la frenata automatica d'emergenza (AEB) possono subire delle limitazioni dovute da eventuali malfunzionamenti dei sensori. Questo contesto evidenzia l'esigenza di un approccio maggiormente integrato dove la comunicazione V2V collabora con i dati provenienti dai sensori. In questo modo si amplia la percezione del veicolo riguardo all'ambiente circostante per poter prevedere e rispondere ad una varietà più grande di situazioni critiche per la sicurezza.

Il termine V2I è riferito alla comunicazione tra veicoli e diversi dispositivi che compongono la rete stradale di un paese. Questi ultimi includono segnali stradali, parchimetri, telecamere, lampioni e delimitatori di corsie. La tecnologia V2I utilizza una rete wireless bidirezionale per inviare dati dagli elementi delle infrastrutture alle auto e viceversa. I sistemi di trasporto intelligente o ITS usano i sensori V2I per raccogliere informazioni e avvisare i conducenti riguardo a disponibilità di parcheggio, ingorghi stradali e condizioni delle strade. Inoltre, V2I è utilizzata nei sistemi di monitoraggio del traffico per stabilire limiti di velocità e modificare la fase e la temporizzazione dei segnali semaforici in modo da incrementare il risparmio di carburante e rendere più efficiente il flusso veicolare.

Un altro strumento è la V2P (Vehicle to Pedestrian) che risulta fondamentale per la tutela degli utenti vulnerabili della strada (VRU). La connessione tra veicolo e pedone può avvenire tramite l'utilizzo di sensori posti sulle infrastrutture della strada oppure con dei sensori sul veicolo che permettano di mandare dei segnali al conducente, in alternativa con il cellulare del pedone sfruttando la connessione wi-fi o la rete del telefono.

Per il rapporto tra smartphone e veicolo, è presente la comunicazione V2D (Vehicle to Device) basata sul protocollo bluetooth. Alcuni esempi sono Android Auto di Google e CarPlay di Apple.

Con la V2C (Vehicle to Cloud) basata sulle reti mobili si possono condividere e archiviare dati sul cloud. Questa tecnologia viene usata per diagnosi del veicolo da remoto, aggiornamenti over the air (OTA) del software del veicolo, comunicazione con gli assistenti digitali e il salvataggio delle preferenze riguardanti posizione del sedile, specchietti e non solo.

Legata al concetto di "Smart City", è presente la V2G (Vehicle to Grid) che consente lo scambio di informazioni tra veicoli elettrici ed ibridi. V2G permette inoltre un utilizzo avanzato dei veicoli elettrici adibiti a fonti energetiche soprattutto in contesti di emergenza come le operazioni di recupero

post-disastro oppure nei periodi di insufficiente disponibilità di elettricità. I veicoli elettrici compatibili con la tecnologia V2G possono operare autonomamente o insieme a sistemi di accumulo già presenti per reintegrare energia nella rete. Questa funzionalità è cruciale per mitigare le sospensioni nella fornitura e garantire la solidità della rete. In aggiunta, V2G permette ai veicoli di accumulare energia quando i prezzi sono bassi e di reintegrarla quando le tariffe aumentano. Grazie alla possibilità di accumulare e restituire energia, i veicoli elettrici con V2G possono avere un peso rilevante nella transizione verso fonti di energia rinnovabile, come quella eolica e solare, le quali sono soggette a fluttuazioni nella produzione.

1.2 Storia

Contrariamente a quello che si potrebbe pensare, la nascita delle connected cars non è estremamente recente, bensì inizia nel 1980 quando la BMW installò per la prima volta un computer di bordo in una monoposto di F1 che permetteva di inviare i dati del veicolo ai box. Quindi le vetture di questo sport rappresentano le precorritrici delle auto connesse per il mercato di massa.

Il passaggio dalla pista alla strada avviene nel 1996, quando General Motors, grazie alla collaborazione con OnStar, presentò tre versioni del modello “Cadillac”, dotate della funzionalità eCall. In caso di collisione, l’apertura degli airbag faceva scattare una chiamata al centro di emergenza. Chiaramente si tratta di un sistema relativamente efficiente in quanto non si poteva avere la certezza che il conducente fosse ancora in grado di comunicare dopo l’incidente.

Nel 1997, Daimler-Benz depositò il brevetto per la chiave intelligente (smart key) e la Mercedes classe S W220 del 1998 fu la prima auto provvista di smart key che consentiva l’apertura e la chiusura delle porte tramite un mini telecomando con due pulsanti.

BMW si conferma precursore della mobilità connessa nel 1998, quando introdusse nel mercato il pacchetto di optional BMW Assist che comprendeva Concierge Service, chiamata di emergenza intelligente e servizio di aggiornamento sul traffico.

Per l’arrivo del GPS all’interno dei veicoli, bisognerà attendere Maggio del 2000, quando Bill Clinton autorizzò l’utilizzo della tecnologia GPS per scopi civili e commerciali mentre precedentemente questa tecnologia era ad uso esclusivo del comparto militare. In questo modo si poterono individuare i veicoli rubati e gli spostamenti divennero più precisi.

L’installazione dei primi dispositivi di diagnostica remota avvenne nel 2001 e permetteva alle case automobilistiche di individuare guasti o errori molto più velocemente.

BMW ritorna ad essere la protagonista nel 2004, con l’introduzione di schede SIM installate nei suoi veicoli. Con questo strumento, gli automobilisti possono ricevere informazioni su meteo, messaggi, notizie ed inoltre monitorare anonimamente le condizioni del traffico.

Grazie al visionario Steve Jobs, nel 2007 avviene la transizione dai cellulari agli smartphone ed esattamente un anno dopo, Crysler rilascerà sul mercato la prima auto con funzionalità hotspot internet per smartphone e Google presenterà al pubblico il sistema operativo Android. Successivamente diverse case automobilistiche inizieranno a immettere sul mercato le loro app.

Nel 2012 arriva il servizio MirrorLink, che consente di utilizzare la funzionalità e la connettività del telefono mediante il sistema di infotainment dell’auto semplicemente collegando lo smartphone all’auto tramite bluetooth oppure porta USB. Sempre lo stesso anno verrà mostrata al pubblico la prima Tesla Model S ed avrà connessione 3G e aggiornamento del software over the air (OTA), ovvero senza l’utilizzo di connessioni fisiche o di azioni manuali.

Due anni dopo, Apple espone al pubblico del Salone di Ginevra la nuova app Apple CarPlay mentre Google mostrerà Android Auto ed entrambi rappresenteranno un’alternativa a MirrorLink e

consentiranno di utilizzare in auto le funzioni dell'Iphone o smartphone Android, grazie al sistema di infotainment della vettura. Sempre nel 2014, Audi e General Motors iniziano a rendere disponibili hotspot 4G per le loro automobili.

Il potenziale delle nuove funzionalità all'interno delle auto comincia ad essere compreso anche dagli enti regolatori; infatti, nel 2015 verrà approvato il regolamento 2015/758 che stabilisce l'obbligo di installazione del sistema eCall all'interno delle auto e dei furgoni leggeri prodotti dal 31 Marzo 2018 in poi. Si tratta di un dispositivo che esegue una chiamata automatica al 112 per inviare informazioni come numero dei passeggeri, posizione del veicolo, alimentazione e tipo di veicolo in modo tale che i soccorsi possano comprendere la situazione e intervenire rapidamente ed efficacemente. Oltre ad emergere il tema della sicurezza sulle strade, inizieranno a presentarsi i primi problemi di cybersecurity. Proprio nel 2015, Charlie Miller e Chris Valasek riuscirono a mettere in atto un attacco informatico da remoto su una Jeep Cherokee tramite il loro PC che gli permise di avere il controllo su radio, aria condizionata, freni, tergicristalli e acceleratore.

Toyota fu tra le prime cause automobilistiche a comprendere il futuro della mobilità e nel 2016 rilasciò sul mercato le prime auto dotate di comunicazione V2X, inizialmente incentrata sullo scambio di dati tra veicolo e infrastrutture (V2I) e tra veicolo e veicolo (V2V), basato su DSCR. Negli USA, Audi annuncia l'introduzione del sistema Traffic Light Information per la comunicazione V2I che consente di segnalare sul quadro strumenti i secondi restanti prima che la luce del semaforo diventi verde.

Nel 2017, Volvo comunica l'inizio di una partnership con Google per sviluppare Android Automotive, un sistema operativo Android per il sistema di infotainment delle auto che con la concessione di un codice comune potrà essere personalizzato dalle case automobilistiche sia da un punto di vista estetico che funzionale. Diversamente da Android Auto, si tratta di un'unità autonoma che permette di gestire il veicolo a 360 gradi senza l'uso del cellulare e possiede Vivaldi, un browser con funzionalità specifiche per l'automotive come la riproduzione di video esclusivamente in modalità audio per contrastare le distrazioni alla guida.

Negli anni a seguire, diversi produttori di automobili e aziende del settore delle telecomunicazioni condurranno esperimenti per l'inserimento della tecnologia V2X all'interno delle automobili.

A partire da Aprile 2018, tutte le nuove automobili dovranno essere dotate del dispositivo eCall.

Con lo scopo di limitare gli incidenti e le morti sulle strade, la commissione Europea approva a fine 2019 il Regolamento 2019/2144 che stabilisce per i nuovi veicoli a motore l'obbligo di equipaggiamento di alcuni sistemi avanzati di sicurezza ADAS a partire da Maggio 2022.

Nel 2020, il sistema operativo Android Automotive ha fatto il suo debutto sul sistema di infotainment della Volvo Polestar 2.

Il 6 Luglio 2022, gli ADAS previsti dal regolamento 2019/2144 diventano obbligatori per i modelli di nuova omologazione.

Viste le possibili opportunità economiche ma anche i problemi di privacy presenti nell'ambito dei dati, il Parlamento Europeo approva il Data Governance Act il 30 Maggio 2022 e il Data Act a fine 2023.

Dal 7 Luglio 2024, i sistemi ADAS del regolamento 2019/2144 sono obbligatori su tutte le autovetture da immatricolare, anche se già prodotte.

1.3 Mercato

Riguardo al mercato delle auto connesse, per i prossimi 6 anni a partire dal 2024, le previsioni mostrano un CAGR del 13,3% con una transizione da 12,4 miliardi di dollari a 26,4 miliardi di dollari.

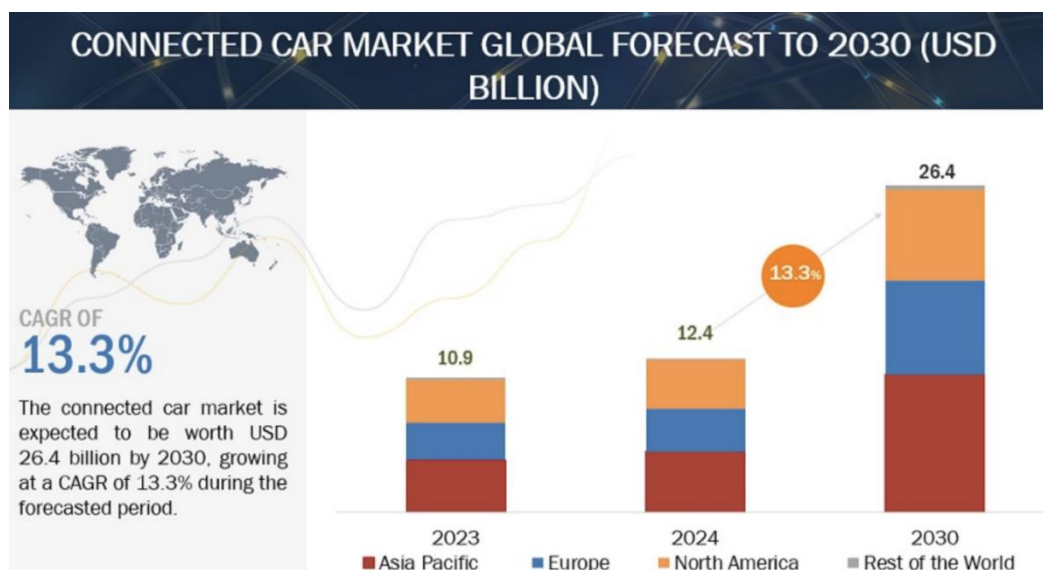


Fig.1-Fonte: <https://www.marketsandmarkets.com/Market-Reports/connected-car-market-102580117.html>

Sono diversi gli elementi che stanno contribuendo a rafforzare questo trend positivo. I governi che incentivano lo sviluppo di infrastrutture di mobilità intelligente e la crescita delle proposte di tecnologie e funzionalità connesse relative a numerosi ambiti come sistemi avanzati per la sicurezza, servizi di intrattenimento e gestione a distanza del veicolo. Anche il crescente interesse per i veicoli a guida autonoma rappresenta una spinta non indifferente per il business delle auto connesse.

In particolare, uno dei maggiori driver è il mercato della telematica che sostenuto dalle domande di connettività e sicurezza, sta favorendo il prosperare del settore delle auto connesse e si prevede il raggiungimento di 750 miliardi di dollari prima del 2030. La telematica permette di ottimizzare la condotta di guida e la sicurezza stradale ed inoltre di adeguare i premi assicurativi attraverso polizze basate sull'utilizzo. Il mercato della telematica automobilistica dovrebbe arrivare a 16,1 miliardi entro il 2030 partendo dai 9 miliardi del 2024 con un tasso di crescita annuale composto del 10,1%.

Per quanto riguarda i segmenti del mercato delle auto connesse, quello della connettività integrata rappresenterà il mercato più grande secondo gli analisti di marketsandmarkets e i motivi risiedono nei vantaggi in termini di contenimento dei costi, conformità ai vincoli normativi e miglioramento delle prestazioni e della sicurezza. Le soluzioni integrate sono utilizzate dai produttori di automobili per soddisfare gli obblighi di legge come il dispositivo eCall per l'Europa e per offrire servizi su piattaforma cloud come, ad esempio, aggiornamenti software e diagnostica da remoto, potenziando l'esperienza al volante.

Il segmento che registrerà la crescita più rapida sarà quello dell'Aftermarket, il quale è utilizzato dai consumatori per aggiungere o customizzare le funzioni di connettività delle loro autovetture. I fornitori propongono una vasta tipologia di prodotti come telecamere, hotspot WiFi e soluzioni di

geolocalizzazione per auto. Tra le aziende che operano in questo segmento ci sono Pioneer e Kenwood che hanno realizzato sistemi di infotainment innovativi, dotati di navigazione GPS, connessione bluetooth e integrazione con smartphone. Chiaramente queste proposte appaiono più convenienti se paragonate all'acquisto di una nuova auto.

La market share più significativa di questo settore sarà quella del segmento delle unità di bordo (Obu o On board unit). Questo elemento è essenziale perché rappresenta il sistema nervoso centrale per veicoli di nuova generazione. Alcune delle sue funzioni sono: collezionare informazioni dai sensori, controllare le prestazioni del motore, la posizione GPS e la pressione degli pneumatici, collegandosi a una piattaforma cloud o a un server centrale. Inoltre, è cruciale per l'impiego degli ADAS. Un ramo della OBU è rappresentato dalla Diagnostica di bordo (On board diagnostics) per la quale si prevede un tasso di crescita annuale composto pari al 54,6% tra il 2024 e il 2030 a livello mondiale.

A livello europeo è presente l'European Transport Safety Council, un'organizzazione internazionale senza scopo di lucro che da diversi anni promuove la distribuzione di tecnologie che permettano di ridurre gli incidenti sulle strade come veicoli autonomi, sistemi di trasporto su richiesta e auto connesse alla rete 5G. Inoltre, l'E.T.S.C. ha evidenziato come la crescente connettività tra le auto sia stimolata dall'utilizzo sempre più diffuso di sicurezza, navigazione, gestione del veicolo e infotainment. Tutto ciò ha influenzato la produzione degli OEM, i quali stanno destinando sempre più risorse alla creazione di funzionalità e tecnologie innovative.

Per quanto riguarda l'Italia, il mercato riguardante connected car & mobility è in continuo aumento come mostrato dall'Osservatorio Connected Car & Mobility del Politecnico di Milano.

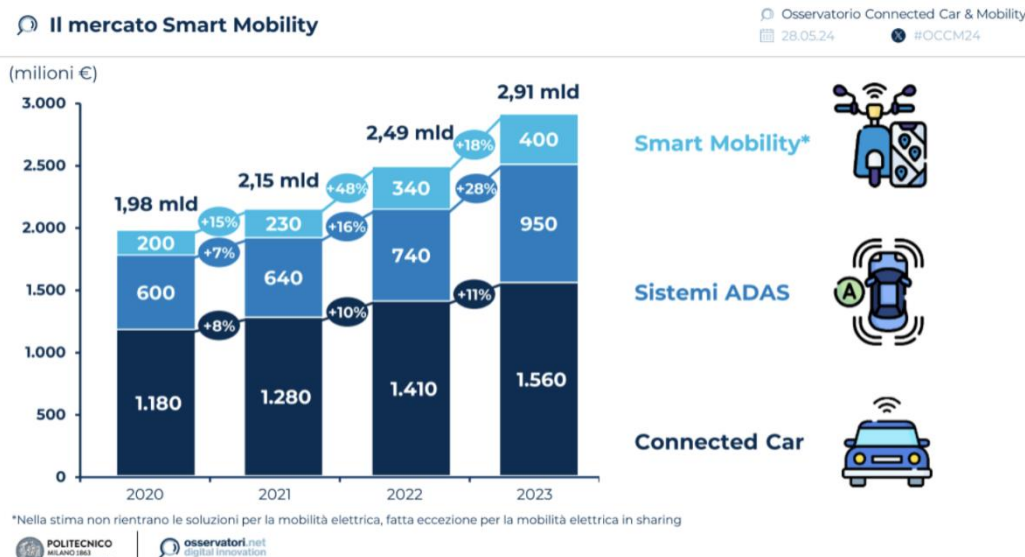


Fig. 2-Fonte: <https://www.economyup.it/automotive/connected-car-mobility-sempre-piu-auto-connesse-soluzioni-sostenibili-e-smart-road/>

Nel 2023 le auto connesse erano 16,9 milioni, poco meno della metà di quelle in circolazione e comprendono 10,3 milioni dotate di scatola GPS/GPRS per monitorare e archiviare i dati di guida a scopo assicurativo in aumento del 3% rispetto al 2022, 1,5 milioni di auto aziendali connesse per la gestione della flotta che registrano un +25% paragonate con il 2022 e 5,1 milioni di auto native connesse tramite Sim card di consumatori privati con un incremento del 19% rispetto al 2022.

Relativamente ai driver del mercato, il direttore dell'Osservatorio Connected Vehicle & Mobility Giulio Salvadori dichiara: "Il settore della mobilità connessa continua a crescere, spinto da innovazioni tecnologiche e novità normative. Sempre più aziende sono in grado di raccogliere grandi quantità di dati da veicoli e infrastrutture connesse, utilizzabili per offrire nuovi servizi di valore. E i risultati si vedono: nel 2023 il fatturato della vendita di servizi è cresciuto del 29%, toccando i 620 milioni di euro. Sul fronte normativo, incide sia l'obbligo a partire dal 2024 di integrare specifici ADAS all'interno di tutte le vetture di nuova immatricolazione che quello dal 2035 di immatricolare solo veicoli a zero emissioni. La connettività avrà un ruolo molto importante nella gestione dei nuovi modelli elettrici e ibridi, e nel garantire scambi di informazioni tra veicolo e infrastruttura".

In una visione più ampia, che comprende anche la smart mobility, nel 2023 il mercato italiano è arrivato a quota 2,91 miliardi di euro, in aumento del 17% se paragonato al 2022. All'interno di questo dato sono inclusi 950 milioni di euro (+28%) relativi ai sistemi di sicurezza avanzati (ADAS), 400 milioni di euro (+18%) riguardanti la mobilità intelligente e 1,56 miliardi di euro (+11%) di soluzioni per l'auto connessa.

Capitolo 2-Stakeholders e dati

2.1 Carmaker

Tutto ha inizio con le case automobilistiche, principali responsabili e supervisori della raccolta di dati relativi a vetture e conducenti. Attualmente esse realizzano delle vetture che sono in grado di supervisionare le strade a 360 gradi, specialmente i modelli a guida autonoma. In considerazione del fatto che queste ultime rappresenteranno il futuro, i sensori sono una componente essenziale per lo sviluppo delle auto sia per la guida che per un abitacolo che si orienta verso una maggiore digitalizzazione e interattività. Ci sono svariate tipologie di sensori in un veicolo, tra cui radar, diverse varianti di LiDAR e videocamere. Inizialmente furono impiegati semplicemente per gli ADAS di base come la videocamera per la retromarcia, con il passare del tempo l'autonomia del veicolo è aumentata portando ad un incremento continuo del numero di sensori. Questi ultimi si possono suddividere nelle seguenti categorie:

- *Videocamera*: è ciò che si avvicina maggiormente alla percezione visiva umana e cattura immagini che in un secondo momento vengono interpretate da sistemi algoritmici. Le immagini acquisite da una videocamera per auto contengono informazioni relative all'ambiente circostante, tra cui altri mezzi, marciapiedi, segnali stradali e utenti vulnerabili della strada. Tramite il processamento da parte dell'algoritmo, si individuano gli ostacoli lungo il percorso al fine di poter attivare ADAS come quello per il mantenimento della corsia.
- *Radar a onde millimetriche*: La sua capacità di "visionare" l'ambiente è superiore rispetto alla telecamera in quanto garantisce alta definizione e performance elevate, oltre che un'ottima capacità direzionale, risultando meno vulnerabile a fenomeni atmosferici o interferenze. Nonostante ciò, per via del notevole costo, è usato solamente per gli ADAS ed inoltre presenta una minore efficacia nel rilevare elementi non metallici.
- *LiDAR*: Sfruttando la luce, il LiDAR emette rapidi impulsi di segnali laser che riflettono sugli impedimenti. Nello specifico, calcola l'intervallo di tempo che un impulso impiega per tornare indietro affinché riesca a determinare in maniera accurata la distanza tra vettura e impedimento. Tramite delle componenti meccaniche, il LiDAR meccanico indirizza un fascio laser. Quest'ultimo presenta dei costi di produzione elevati ma garantisce una visione a 360 gradi, maggiore precisione e possiede un raggio d'azione superiore. La versione a stato solido del LiDAR risulta più economica e utilizza prevalentemente elementi elettronici per controllare l'angolo di diffusione del laser ma possiede degli angoli di scansione più ridotti ed è meno accurato.
- *LiDAR 3D Time of Flight*: Questa è un'altra variante di LiDAR che può gestire diverse applicazioni per il rilevamento a corto raggio nel settore automotive, non utilizza uno scanner e può ottenere un grado di precisione maggiore. Inoltre, è sempre più diffuso in numerosi dispositivi, inclusi gli smartphone, nei quali permette di calcolare distanza e volume grazie a impulsi ottici di breve durata e elevata intensità al fine di ottenere dati relativi alla profondità su distanze ravvicinate. In conclusione, il LiDAR 3DToF è in grado di mappare e monitorare oggetti, assistere il rilevamento di gesti e altimetri sensibili, oltre a generare una panoramica a 360 gradi al di fuori del veicolo migliorando le manovre di parcheggio.

Con l'incremento della digitalizzazione degli interni, i sensori precedentemente mostrati assumono importanza anche nell'abitacolo. Il LiDAR a corto raggio d'azione può controllare le condizioni del guidatore e degli altri occupanti per agevolare l'implementazione di funzioni avanzate quali l'identificazione del volto con lo scopo di adattare le impostazioni personalizzate, i comandi gestuali senza contatto e il potenziamento del display head up che proietta sul parabrezza delle immagini contenenti informazioni utili per la guida, come la velocità corrente del veicolo e i limiti vigenti su quel tratto di strada.

Riguardo alla tecnologia di rilevamento dei comandi gestuali, i movimenti umani rappresentano degli input che vengono captati da sensori e telecamere. Successivamente, tecnologie di machine learning supportate da algoritmi e IA esaminano i gesti e li convertono in comandi. Il conducente potrebbe compiere numerose operazioni basilari, come il controllo della temperatura interna e del volume audio tramite il riconoscimento dei gesti invece che con comando vocale o tocco. Sempre con questa tecnologia, si possono individuare eventuali segnali di stanchezza o distrazione del guidatore.

Oltre alla tecnologia LiDAR, anche i sensori radar ad onde millimetriche sono utilizzati per i comandi gestuali in quanto offrono una maggiore precisione e sono più performanti rispetto alle telecamere perché riescono ad identificare e riconoscere più occupanti nell'abitacolo, anche attraverso diversi materiali e circostanze ambientali impegnative. Oltre a ciò, sono in grado di differenziare un bambino da un adulto al fine di regolare lo sblocco dell'airbag e di individuare possibili estranei all'esterno del veicolo. Una funzionalità più evoluta è il controllo del battito cardiaco e del ritmo respiratorio.

Esistono vari metodi per monitorare veicoli e conducenti:

- *Localizzazione della posizione* - I sistemi GPS incorporati permettono di localizzare con precisione la posizione del veicolo in qualsiasi momento. Le varie finalità riguardano abitudini di viaggio dei conducenti e percorsi.
- *Preferenze dei conducenti* - Comprendono la memorizzazione dell'assetto del sedile, le preferenze di intrattenimento e il sistema di climatizzazione per offrire un'esperienza al volante su misura.
- *Ambiente circostante* - Dati che riguardano ad esempio le condizioni dell'aria, lo stato delle strade e la temperatura per ottimizzare il controllo dell'ambiente esterno, la sicurezza attiva e/o passiva e le funzionalità di guida assistita.
- *Stile di guida* - Monitoraggio di parametri come movimento dello sterzo, intensità della frenata, dell'accelerazione e velocità.
- *Dispositivi connessi* - In base alla casa automobilistica, l'auto può essere in grado di interagire e acquisire dati da device mobili connessi come lo smartphone per accedere a messaggi, chiamate, uso delle applicazioni e così via. Non a caso, sono diverse le case automobilistiche che hanno rilasciato la loro app.
- *Airbag* - Si tratta di dati che includono la massa e la seduta del passeggero per identificare criticità nella vettura e analizzare le dinamiche dei sinistri.
- *Dati generali sul veicolo* - Sono presenti una moltitudine di sensori che forniscono informazioni sullo stato del veicolo come la pressione degli pneumatici, la temperatura del motore, livello del liquido di raffreddamento, livello del carburante, la pressione dell'olio e non solo.

- *Intrattenimento* - Informazioni riguardanti l'uso delle funzionalità del sistema di infotainment come applicazioni, radio, piattaforme di streaming e navigazione.
- *Consumo di energia in casa* - Nel momento in cui un veicolo elettrico viene collegato ad un sistema di ricarica domestico, l'auto è in grado di raccogliere informazioni sulla routine di ricarica e sui consumi energetici.
- *Traffico Wi-Fi* - Le auto possono registrare l'uso della connessione Wi-Fi e ottenere informazioni sulla navigazione in internet.
- *Caratteristiche biometriche* - Qualche vettura è anche in grado di collezionare dati fisiologici come impronte e volto che vengono impiegate per scopi di sicurezza come l'accesso al veicolo o l'accensione del motore.
- *Rilevamento vocale* - Grazie alla tecnologia di riconoscimento vocale, si possono gestire varie funzionalità del veicolo usando semplicemente la propria voce.
- *Comunicazioni di allarme* - I veicoli recenti, possono emettere notifiche riguardanti sicurezza e furto che vengono mandate sullo smartphone.

I produttori di apparecchiature originali (OEM) usano i dati ottenuti dai vari sensori posti sulle auto per modernizzare l'esperienza di guida e sviluppare vetture in grado di tutelare maggiormente la salute delle persone a bordo. Le tecnologie dei sensori attuali sono in grado di trasformare profondamente l'esperienza al volante. Grazie ai dati provenienti dai sensori e all'uso di tecnologie all'avanguardia, gli OEM possono realizzare automobili innovative, migliorando al tempo stesso l'elaborazione e la memorizzazione dei dati.

Gli stessi consumatori ricevono supporto tramite le informazioni dei sensori per mantenere in ottime condizioni le loro automobili. D'altro canto, gli OEM sfruttano questi dati per potenziare attività come il controllo delle condizioni del veicolo, soccorso stradale e manutenzione.

Per esempio, gli OEM possono sviluppare i veicoli integrando elementi di manutenzione predittiva. I sensori supervisionano costantemente lo stato meccanico e nel momento in cui si individua un'anomalia, il guidatore riceve una notifica che spiega la natura del guasto e il tempo entro cui è consigliato far revisionare il veicolo.

In aggiunta, i produttori di parti originali possono cooperare con i servizi di soccorso stradale per rendere più efficiente e rapido l'intervento in caso di sinistro. Questo avviene già tramite il dispositivo *eCall*, la cui installazione è stata resa obbligatoria dal 31 Marzo 2018 su tutte le nuove automobili e i furgoni leggeri. Quando i dispositivi di rilevamento avvertono un impatto considerevole, il sistema chiama in maniera automatica il 112 per stabilire una comunicazione vocale con il centro di emergenza e trasmettere le informazioni riguardanti l'incidente come la posizione GPS, l'orario, l'identificativo del mezzo e il senso di marcia. Utilizzando un pulsante specifico, la chiamata può partire manualmente e questo risulta particolarmente utile se si assiste ad un sinistro.

Sempre in tema di guida sicura, gli *ADAS* rientrano tra i protagonisti in quanto sulla base del Regolamento 2019/2144, le automobili di nuova immatricolazione dovranno possederne alcuni e da 2 anni sono già obbligatori sulle vetture di nuova omologazione. Comprendono diversi elementi di sicurezza attiva che integrano i sistemi di sicurezza passiva dei passeggeri e assistono il guidatore semplificando l'utilizzo della vettura.

Di seguito gli ADAS in dettaglio.

Monitoraggio della concentrazione del conducente - Sfruttando dei sensori che controllano l'uso e i movimenti del volante, è possibile accertare la stanchezza del guidatore. In questa situazione, apparirà un messaggio sul display dietro al volante che suggerirà una pausa al fine di prevenire la sonnolenza. In futuro questo sistema sarà più evoluto con la registrazione del battito delle palpebre tramite telecamera. Questa funzionalità non è attualmente disponibile per questioni di privacy e l'obbligo è stato rinviato al 2026.

Mantenimento della corsia - Questo sistema opera tra 65 e 130 km/h, attraverso una videocamera in grado di individuare le linee bianche che delimitano la corsia: se il conducente dovesse effettuare un cambio di corsia senza gli indicatori di direzione, il sistema entra in funzione e riporta l'auto nei limiti della corsia usando automaticamente lo sterzo.

Controllo dell'area posteriore in retromarcia - Consente di individuare oggetti situati dietro al veicolo nel corso della manovra di retromarcia tramite videocamera o sensori. Il regolamento europeo non richiede una specifica tecnologia, ma diverse case automobilistiche preferiscono installare la videocamera posteriore.

Frenata automatica - Basato su sensori radar e telecamere, questo dispositivo identifica la presenza di utenti vulnerabili della strada e allerta il guidatore. Se non viene registrata una qualche reazione da parte di quest'ultimo, il sistema entra in funzione attivando i freni per prevenire la collisione. Opera tra i 10 e i 60 km/h ed è in grado di evitare l'impatto per velocità inferiori ai 40 km/h in condizioni di superficie stradale asciutta e con temperatura compresa tra 0 e 45 °C.

Panic Stop - Se si verifica una frenata improvvisa, indipendentemente dal fatto che sia effettuata dal conducente o dal sistema elettronico di frenata automatica, questo dispositivo attiva l'illuminazione intermittente delle luci di stop per segnalare l'evento anche alle vetture al seguito.

Assistenza intelligente alla velocità - Serve per segnalare al conducente i limiti di velocità lungo il tragitto, i quali sono individuati tramite le informazioni fornite dal sistema di navigazione e da una telecamera. Anche in questo caso, il produttore è libero di scegliere tra 3 modalità di segnalazione: visivo e acustico, visivo con vibrazione o solo vibrazione. In alternativa può attivare una decelerazione del veicolo per adeguarsi ai limiti.

Modulo di collegamento per alcolock - Alcolock è un dispositivo che blocca l'accensione del veicolo se individua un tasso alcolemico oltre il limite consentito dalla legge. La sua presenza a bordo non è obbligatoria secondo la normativa dell'UE, ma impone che il veicolo sia progettato per un'installazione semplice e veloce, conformandosi ad uno standard comune.

Event Data Recorder - "Registratore di dati di evento" è il termine utilizzato nella versione italiana del regolamento europeo 2019/2144. Si tratta di un dispositivo erroneamente chiamato Scatola nera, in quanto risulta differente rispetto a quello fornito dalle compagnie assicurative. La definizione è la seguente: "Un sistema progettato esclusivamente al fine di registrare e memorizzare i parametri relativi agli incidenti e le informazioni immediatamente prima, durante e immediatamente dopo una collisione". Di fatto, il suo scopo non è quello di conservare dati relativi alla guida ordinaria e non

può registrare video o audio. Funziona in maniera automatica, deve essere integrato nel veicolo sin dalla fase di progettazione, non può essere disabilitato dal conducente e archivia dati esclusivamente nel momento in cui si manifesta una collisione. I suddetti dati rimangono all'interno del dispositivo in quanto non possono essere trasmessi all'esterno vista l'assenza di connessione bluetooth, satellitare o wifi. Di conseguenza, non è in grado di determinare né la posizione del veicolo né quella dell'incidente. L'intento della normativa prevede come fine ultimo quello di utilizzare i dati "per effettuare analisi sulla sicurezza stradale e valutare l'efficacia delle specifiche misure adottate senza permettere di identificare il proprietario o il titolare di uno specifico veicolo". Pertanto, non sono destinati a stabilire le colpe nell'eventualità di un sinistro come si potrebbe immaginare, ma l'articolo 6 al punto 4d) riporta che "i dati che sono in grado di registrare possono essere messi a disposizione delle autorità nazionali, mediante un'interfaccia standardizzata, in base alla legislazione nazionale o dell'Unione, soltanto ai fini della ricerca e dell'analisi in relazione all'incidente".

Le informazioni dei sensori possono offrire indicazioni preziose ai team di Ricerca e Sviluppo per capire con maggiore precisione le necessità e gli interessi dei guidatori.

La gestione dello spazio di memorizzazione e dell'analisi dei dati rappresenta uno dei più importanti ostacoli che gli OEM stanno affrontando. L'edge computing rappresenta una tecnologia di grande potenziale poiché consente l'analisi delle informazioni direttamente sul luogo di raccolta invece di inviarli al cloud per l'elaborazione. Con questa modalità, si ottengono esiti e feedback più tempestivi elevando il comfort alla guida. Quindi si parlerebbe di una soluzione che integra l'edge computing con il cloud storage e quest'ultimo verrebbe usato esclusivamente per quei dati da conservare per un periodo prolungato.

2.2 Assicurazioni

Il rapido sviluppo dell'Internet of Things e l'ampia diffusione di dispositivi di rilevamento stanno creando un volume consistente di dati che integrati con metodi di analisi avanzata e strumenti di big data, stanno aprendo nuove opportunità per progettare prodotti innovativi e cambiare il metodo con cui vengono prese le decisioni riguardo a prezzi e risk management in vari settori come quello assicurativo. Queste tecnologie hanno stimolato la creazione di polizze basate sull'utilizzo (*Usage-Based-Insurance* o *UBI*) che monitorano i chilometri percorsi e lo stile di guida.

Nello specifico, tramite l'uso di dispositivi telematici e applicazioni mobili si raccolgono dati che permettono di calcolare più accuratamente il premio in modo tale che rifletta il rischio effettivo. L'aspetto fondamentale per determinare quest'ultimo consiste nell'adattare il suo valore all'analisi evolutiva del profilo assicurativo. In questo modo i guidatori sono incoraggiati a modificare il loro stile di guida per ottenere un canone assicurativo più contenuto. Le strutture tariffarie dei programmi UBI rispecchiano l'assicurazione imparziale, nella quale i conducenti considerati a basso rischio pagano meno mentre quelli a rischio elevato sostengono una spesa superiore. Infatti, i clienti più apprezzati dalle assicurazioni sono quelli con un profilo di rischio ridotto, in grado di produrre utili stabili per l'azienda. Coloro che hanno un elevato livello di rischio compromettono sia la loro sicurezza che i margini di profitto dell'assicurazione ed i costi legati ad un sinistro sono maggiori dei profitti. Di conseguenza, tra gli obiettivi dell'assicuratore rientrano l'individuazione dei profili a rischio elevato e la condivisione di suggerimenti per aiutarli a correggere le abitudini di guida.

La scelta di rilasciare dei feedback dopo un viaggio risulta capace di apportare miglioramenti significativi nella condotta al volante poiché offrono quotidianamente o settimanalmente suggerimenti o avvisi ai guidatori al termine del loro spostamento tramite report di viaggio, premi o valutazioni, con l'intento di promuovere comportamenti di guida sicuri. Nello specifico:

- *Resoconti di viaggio* - Si tratta di report storici disponibili su piattaforme online o forniti su carta e che comprendono statistiche e informazioni dettagliate sui tragitti. Solitamente sono presenti anche delle comparazioni con altri conducenti come fonte di stimolo per un miglioramento della condotta al volante tramite lo spirito competitivo.
- *Premi* - Di solito sono associati allo stile di guida o integrati con sistemi di punteggio.
- *Mappa delle abitudini di guida* - Unendo i resoconti di viaggio con le mappe, gli assicurati ricevono un riscontro visivo per le zone nelle quali hanno mostrato condotte rischiose in modo da poter adottare una guida più cauta su quei tratti per il futuro. In altre parole, i guidatori potrebbero ricevere una mappa che segnala le zone con alta frequenza di eventi rischiosi in modo da evitare queste aree, scegliendo strade diverse oppure adottando precauzioni specifiche.
- *Punteggio* - Si tratta di punteggi assegnati in base alle abitudini di guida dell'assicurato, il quale li può confrontare con le performance passate al fine di ottimizzare la sua condotta e incrementare la sua valutazione.

Ciò nonostante, queste misure non forniscono in maniera automatica dei consigli su misura per ogni assicurato perché è necessario analizzare i fattori che influenzano il rischio associato all'assicurato.

Facendo un confronto con le classiche polizze, tra le variabili tipicamente utilizzate per stabilire i costi della polizza, sono presenti l'uso giornaliero e stagionale, le condizioni meteo, il chilometraggio, la posizione, la distanza di pendolarismo e altre informazioni su vettura e guidatore. Il problema risiede nel fatto che la loro attendibilità è legata alla veridicità o meno delle dichiarazioni fornite dai clienti al momento della stipula.

Il progresso tecnologico, l'aumento dell'interesse per i servizi di connettività a bordo e la disponibilità degli assicurati a fornire i propri dati hanno contribuito ad un crescente ampliamento dei programmi UBI. Questi comprendono polizze legate al chilometraggio del veicolo conosciute come *Pay-As-You-Drive* o *PAYD*, quelle basate sullo stile di guida del conducente chiamate *Pay-How-You-Drive* o *PHYD* e altre che non si limitano a riduzioni sui premi, ma offrono soluzioni a valore aggiunto e incentivi specifici per promuovere la fidelizzazione dei clienti e incrementare la competitività note come *Pay As You Drive As You Save* o *PAYDAYS*. Gli attuali strumenti di telematica permettono di monitorare fattori chiave come le località in cui il veicolo viene utilizzato, la fase del giorno (se diurna o notturna), l'intensità di accelerazione, la frenata e l'uso dello sterzo.

Le motivazioni dietro la maggiore attenzione per l'uso della telematica derivano dai vari benefici ottenuti dagli assicurati e dagli enti assicurativi. Questi ultimi ottengono vantaggi che consistono in una stipula e una stima economica del rischio più accurate, nella diminuzione dei costi legati ai reclami, nell'abbassamento della severità dei sinistri, nella mitigazione dei comportamenti opportunistici e dell'asimmetria informativa, nel rafforzamento della riconoscibilità e della lealtà al marchio e nel cambiamento delle condotte rischiose. Mentre per quanto riguarda i clienti, gli aspetti positivi includono premi potenzialmente più vantaggiosi, una procedura di richiesta di indennizzo migliorata, soccorso stradale, diagnostica a distanza, prontezza nelle emergenze, servizi di rintracciamento delle vetture rubate e maggiore sicurezza in generale.

Inoltre, anche la stessa comunità può essere influenzata positivamente dalla diffusione di polizze UBI poiché contribuiscono a diminuire le esternalità negative associate a sinistri e utilizzo delle autovetture da parte di consumatori privati. Ad esempio, riduzione di consumi, sinistri e congestione stradale, emissione di gas inquinanti minore grazie a tragitti più brevi, oltre ad una guida più responsabile.

Per quanto riguarda i dispositivi usati dalle compagnie assicurative per raccogliere dati, ne sono presenti 3 tipi: scatola nera, dispositivo plug and drive e app per smartphone.

La *black box* è un apparecchio elettronico costruito con materiali in grado di resistere a forti impatti e progettato per raccogliere e memorizzare specifiche informazioni in un archivio. Tipicamente è costituita da un sensore GPS integrato al suo interno che riesce a tracciare la velocità, la distanza percorsa e il senso di marcia, un accelerometro per la forza di frenata e potenziali collisioni, una scheda SIM per collezionare i dati e un software per computer che verifica il modo in cui le informazioni vengono elaborate e trasferite. Il montaggio viene effettuato da un centro di assistenza convenzionato con l'ente assicurativo e prevede l'installazione della scatola nera in parti non visibili all'interno dell'abitacolo.

Sia le Forze dell'Ordine che le stesse compagnie assicurative usufruiscono della scatola nera per analizzare le circostanze di un sinistro e stabilire possibili colpe, oltre che a monitorare nel tempo lo stile di guida del conducente.

È importante evidenziare che la black box può memorizzare soltanto gli avvenimenti riguardanti un incidente e i dati operativi del veicolo.

In dettaglio, i dati trattati riguardano:

- Posizione del veicolo tramite GPS
- Tempi di movimento e di fermata
- Distanze percorse in chilometri
- Tipologia di strada (urbana, extraurbana, autostradale)
- Orari in cui il veicolo è utilizzato
- Collisioni: per ciascun incidente vengono registrati la posizione esatta dell'accaduto, l'orario e la data, il picco di accelerazione, la velocità d'impatto e quella nei momenti precedenti.
- Analisi del comportamento al volante del conducente in funzione della ripetitività storica di accelerazione e frenate improvvise, dei regimi del motore, dell'utilizzo del cambio e delle marce inserite.

Un'altra opzione analoga ad una black box è il *dispositivo plug and drive* che viene collegato all'ingresso USB della vettura, all'adattatore da 12V oppure al connettore OBD e in questo modo il conducente può installarlo in totale autonomia.

La terza alternativa è l'*app per smartphone* che si serve dell'ampia varietà di sensori integrati negli smartphone dei conducenti, i quali sono normalmente presenti nei tradizionali strumenti telematici. Oltre al sistema GPS e all'accelerometro, sono presenti il giroscopio che supporta l'accelerometro nello stabilire il senso di marcia e il magnetometro che determina la posizione del Nord e contribuisce all'identificazione della posizione e del senso di movimento collaborando con GPS e accelerometro. Non solo l'installazione di un'app risulta molto più semplice in quanto non richiede l'intervento di un operatore specializzato ma consente anche un agile accesso ai propri dati sulla guida. Altri vantaggi sono la portabilità in quanto il cellulare può essere facilmente trasferito da un'auto all'altra e l'assenza di vincoli di compatibilità.

Oltre a rilevare informazioni sullo stile di guida del conducente, può accrescere la partecipazione dell'assicurato. Tramite essa i clienti possono ricevere feedback sulla guida e aggiornamenti su premi ottenuti e prossimi obiettivi. Al termine di ogni viaggio, possono esaminare le loro performance al volante e scoprire come migliorare per ottenere premi futuri.

Risulta facilmente intuibile come quest'ultima soluzione presenti evidenti limiti. In primis, la varietà di piattaforme e sistemi operativi come Android, iOS e non solo che nel tempo sono sottoposti a continui cambiamenti. In aggiunta, i sensori di fascia consumer che non sono sviluppati per collezionare dati in ambito telematico e il fatto che ogni smartphone ha delle tecnologie e caratteristiche specifiche che lo differenziano dagli altri. Infine, contrariamente ad una black box, il

telefono si può muovere tranquillamente ed una sua caduta dal sedile potrebbe essere interpretata in maniera errata come un sinistro.

2.3 Gestori delle flotte

Incluso nel contesto della smart mobility è presente il *fleet management* che rappresenta il controllo di mezzi commerciali al fine di migliorare tutto ciò che riguarda la logistica e la mobilità, comprese le soluzioni di car sharing.

Sfruttando la telematica, risulta più semplice ottenere dati relativi a consumi, velocità e non solo al fine di poter identificare il momento ideale per la manutenzione e la riparazione. Inoltre, anche i sensori giocano un ruolo essenziale in quanto permettono di collezionare preziose informazioni per individuare possibili guasti e migliorare sia l'efficienza dei percorsi che la durata operativa dei veicoli.

L'IoT e la connettività sempre più presenti nei veicoli, possono contribuire alla risoluzione di numerose sfide con cui responsabili e manager devono misurarsi per garantire servizi di alto livello, sicuri e fidati. In particolare:

- *Sorvegliare il conducente* - Oltre a verificare le condizioni del veicolo, si può osservare lo stile di guida del conducente per individuare potenziali comportamenti a rischio come velocità oltre i limiti, frenate improvvise o deviazioni dalla corsia.
- *Controllo della temperatura* - Si possono creare sistemi innovativi per gestire carichi che necessitano di un attento controllo della temperatura come nel caso di cibi e farmaci. Di conseguenza, si riesce a proteggere l'interezza del carico fornendo un'esperienza positiva e soddisfacente al cliente.
- *Localizzazione delle risorse* - Molto utile nel caso dei camion che spesso trasportano container e attrezzature varie, consente di evitare furti e smarrimenti assicurando un livello di affidabilità superiore nella gestione delle risorse aziendali.
- *Gestione a distanza del veicolo* - Grazie all'IoT e alle tecnologie innovative di connettività si possono realizzare strumenti per la gestione da remoto di alcuni elementi del veicolo come la possibilità di spegnere il motore nel caso in cui il mezzo venga rubato.
- *Manutenzione predittiva* - Monitorando costantemente parametri cruciali del veicolo, si può dedurre il momento corretto per la manutenzione per prevenire possibili guasti e ridurre al minimo i tempi di inattività del veicolo. Di conseguenza si ottengono vantaggi che riguardano l'abbattimento dei costi e l'ottimizzazione dei processi aziendali.
- *Localizzazione della flotta* - Sfruttando dispositivi dotati di tecnologia GPS si possono raccogliere informazioni dettagliate sulla posizione per migliorare la pianificazione dei tragitti ed ottenere aggiornamenti in tempo reale sulle condizioni del traffico. In questo modo il trasporto sarà maggiormente produttivo e meno costoso.
- *Controllo del carburante* - L'analisi dei consumi di carburante permette di individuare eventuali disfunzioni operative in modo tale da risparmiare sui costi e diminuire l'impronta ecologica.
- *Sistemi di registrazione digitale* - Le informazioni raccolte possono mostrare precisamente le ore lavorative dei guidatori al fine di migliorare la programmazione delle pause. I sistemi applicati per questi scopi sono utilizzati per soddisfare i vincoli normativi che regolano le condizioni di lavoro dei dipendenti

2.4 Mercato europeo dei Machine Data

Il termine *machine data* si riferisce all'enorme volume di dati generati costantemente da macchine e attrezzature industriali. Questa tipologia di dati possiede notevole capacità nel rendere produzione e gestione maggiormente efficienti, sviluppare macchinari innovativi e con elevate performance ed infine creare dei prodotti meno costosi e di qualità superiore. I machine data si trovano al centro dell'attenzione grazie agli ultimi progressi tecnologici, tra cui l'intelligenza artificiale, la tecnologia 5G e l'Internet of Things, arrivando a sorpassare i dati personali in riferimento a valore economico e dimensioni.

I machine data sono conosciuti anche come *dati non personali* o *industriali*. I *dati non personali* rappresentano dati elettronici privi di elementi che permettano di individuare una persona. Per quanto riguarda i dati personali, possono essere convertiti in non personali tramite l'attuazione di tecniche che consentono di anonimizzare i dati, come randomizzazione, mascheramento e generalizzazione.

Nello specifico esistono diverse tipologie di machine data, tra cui:

- *Dati dei sensori* - I sensori vengono tipicamente collocati all'interno di componenti cruciali delle macchine al fine di monitorare il loro stato ed effettuare la manutenzione nel momento ideale. Inoltre, collaborano tra loro per rilevare e acquisire machine data in maniera costante;
- *Dati del registro delle chiamate* - Con il termine 'registro chiamate' si intende quel processo automatico di acquisizione, registrazione e analisi dei dati riguardanti le telefonate. All'interno del registro si possono trovare la durata della conversazione telefonica, sia l'orario di inizio che quello di fine, la localizzazione geografica di colui che effettua la chiamata e di chi la riceve, oltre alla rete impiegata;
- *Dati del web log* - In questo caso si tratta della registrazione delle attività svolte su internet da parte di un utente. Alcuni machine data che rientrano in questa categoria sono indirizzi IP, download e URL di riferimento.
- *Dati dell'application log* - Corrisponde ad un file che registra le operazioni eseguite in un'applicazione software. A titolo di esempio, sono inclusi dati riguardanti l'applicazione di interesse, ID dell'utente, dimensioni dei file scaricati o caricati e periodi temporali di inattività. Le finalità di questo registro sono relative all'analisi e prevenzione del ripetersi di eventuali errori, oltre che monitorare l'attività di varie persone.
- *Dati di computer o system log* - All'interno dei computer vengono prodotti dei file di registro, i quali contengono indicazioni sull'operatività del sistema. Più in dettaglio, un file di registro contiene diverse righe che descrivono operazioni di sistema, inclusa cancellazione o salvataggio di un file, l'accesso ad una rete Wi-Fi, l'avvio di un'applicazione e l'associazione ad un dispositivo bluetooth.

Ci sono state varie tendenze che hanno influenzato il sorgere e la crescita dell'economia dei dati non personali/industriali all'interno dell'Unione Europea. In primis, la più rilevante è stata la trasformazione digitale che ha investito l'industria e la produzione e che ha spinto la Commissione Europea a focalizzarsi su una strategia per i dati allo scopo di potenziare l'economia digitale europea. Questa strategia ha stabilito un sistema di governance a sostegno del mercato dei dati industriali,

evidenziando il bisogno essenziale della condivisione dei dati non personali per lo sviluppo dell'economia digitale europea.

Il dipartimento europeo per le politiche economiche, scientifiche e della qualità della vita ha condotto un'analisi per quantificare il mercato dei dati non personali. In questo studio sono stati considerati otto settori, utilizzando i dati che provengono dall'European Data Market Monitoring Tool. Si tratta di una piattaforma che distribuisce informazioni relative all'economia europea dei dati, inclusi dimensioni del mercato, principali player e cambiamenti o sviluppi. La sua finalità è quella di sostenere lo sviluppo di norme fondate su dati concreti e di supportare le imprese nel processo decisionale in modo tale che prendano decisioni informate nel mercato dei dati. La suddetta analisi è focalizzata su quattro indicatori: quota di monetizzazione dei dati, il numero di fornitori di dati, il numero di professionisti dei dati e la stima annuale del valore dell'economia dei dati. I risultati dell'analisi si trovano nella seguente tabella.

Sector/ EU Data Space	Share of Data Monetisation		Number of data suppliers		Number of Data Professionals (000s)		Data Economy EUR (Bn)	
	2020	2025	2020	2025	2020	2025	2020	2025
Agriculture	0.3%	0.2%	27	83	35	44	2,471	3,131
Finance	28.8%	23.4%	4,621	13,022	609	769	100,500	144,498
Health	3.9%	3.9%	3,101	9,207	518	668	17,269	25,703
Mining, Manufacturing	22.5%	22.8%	21	347	745	945	90,100	127,738
Professional services	15.9%	14.9%	67,958	103,218	1,385	1,820	39,230	60,816
Public Administration	5.9%	7.9%	n/a	n/a	395	485	50,601	89,734
Mobility	4.3%	4.5%	117	412	197	244	16,798	25,090
Utilities	2.6%	2.8%	261	883	92	113	16,782	32,628

Fig.3-Fonte: The emergence of non-personal data markets

Nella successiva tabella sono presenti il tasso di crescita annuale composto (CAGR) e una classifica dei settori basata sul contributo del valore aggiunto lordo del singolo settore all'economia dell'UE.

Sector/EU Data Space	Share of Data Monetisation		Number of data suppliers		Number of Data Professionals		Data Economy	
	2025 ranking*	CAGR	2025 ranking*	CAGR	2025 ranking*	CAGR	2025 ranking*	CAGR
Agriculture	8th	-7.79%	7th	25.18%	8th	4.68%	8th	4.85%
Finance	2nd	-4.07%	2nd	23.02%	3rd	4.78%	2nd	7.53%
Health	6th	0.00%	3rd	24.31%	4th	5.22%	7th	8.28%
Mining, Manufacturing	1st	0.27%	6th	75.24%	2nd	4.87%	1st	7.23%
Professional services	3rd	-1.29%	1st	8.72%	1st	5.61%	4th	9.16%
Public Administration	4th	6.01%	8th	n/a	5th	4.19%	3rd	12.14%
Mobility	5th	0.91%	5th	28.63%	6th	4.37%	6th	8.35%
Utilities	7th	1.49%	4th	27.60%	7th	4.20%	5th	14.22%

Fig.4-Fonte: The emergence of non-personal data markets

Quando si parla di utilizzo di dati non personali, le attività estrattive e manifatturiere rappresentano senza ombra di dubbio un settore strategico; infatti, risulta essere il settore più rilevante in termini di economia dei dati e quota di monetizzazione dei dati. Nonostante le dimensioni di questo settore, il numero di fornitori di dati era piuttosto esiguo nel 2020, ma si stima che crescerà in modo esponenziale entro la fine del 2025 con un CAGR del 75%.

Un altro settore di punta per l'impiego dei dati non personali è quello della finanza. Nonostante una lieve diminuzione della quota di monetizzazione, si stima una crescita simile in media per il suddetto settore. Quest'ultimo, oltre ad essere uno dei più avanzati, presenta notevoli opportunità come evidenziato dalle posizioni nel ranking 2025 dei quattro criteri.

Il settore dei servizi professionali possiede una certa esperienza nell'impiego dei dati non personali. In particolare, vanta il maggior numero di fornitori e professionisti dei dati, con una previsione di crescita costante per gli anni a venire.

Riguardo alle pubbliche amministrazioni, esse otterranno significativi benefici tramite un utilizzo più esteso dei dati non personali. La quota di monetizzazione e l'economia dei dati sono i fattori che registreranno l'incremento più elevato del CAGR con valori rispettivamente del +6% e +12%.

Tra i settori compresi nello studio, l'agricoltura è quello che otterrà minori benefici dai dati non personali. Dal 2020 al 2025, la monetizzazione subirà un calo dello 0,1%. Nonostante ciò, l'incremento del numero dei fornitori e di quello dei professionisti è in linea con gli altri settori.

Dai risultati dell'analisi, si evince che il campo sanitario crescerà in maniera rilevante tra il 2020 e il 2025. Nello specifico, la quota di monetizzazione resterà invariata anche se il valore degli altri indicatori potrebbe aumentare con un andamento analogo a quello degli altri settori.

Relativamente al settore della mobilità, si prevede che registrerà un incremento nell'utilizzo dei dati non personali tra 2020 e 2025. Inoltre, avrà il secondo tasso di crescita più elevato in termini di CAGR per quanto riguarda il numero di fornitori di dati.

Un tasso di crescita comparabile a quello del settore della mobilità sarà registrato dalle utilities (compreso il mercato energetico). L'impiego dei dati non personali sarà esteso e si stima che quello delle utilities, sarà il settore con il più elevato tasso di crescita in termini di CAGR, sostenendo in modo significativo l'economia dei dati dell'UE.

2.5 Mercato europeo dei dati

Il *mercato complessivo dei dati* viene definito dallo “European Data Market study 2021-2023” come “il mercato in cui i dati digitali vengono scambiati come ‘prodotti’ o ‘servizi’ a seguito dell’elaborazione di dati grezzi.”. Nel 2023, il mercato europeo ha raggiunto 81,9 miliardi di euro, registrando una crescita dell’11,1% se confrontato con i 73,8 miliardi del 2022. Nonostante lo scarso impatto dell’AI generativa data la recente nascita del suo mercato, lo sfruttamento dei dati ha visto una rapida crescita nel corso del 2023. In un’ottica di lungo periodo, l’AI generativa inciderà in maniera più significativa su questo mercato, anche se la maggior parte delle spese riguarderà la stessa AI generativa e non altre tecnologie legate ai dati. L’incremento atteso della spesa prevista per l’AI è già incluso in questo mercato e riguarda sistemi di interazione con i clienti, soluzioni per la gestione aziendale e software di dati.

N.	Market	Name	Description	2021	2022	2023	Growth 2022-2023
4.1	EU27	Value of the Data Market	Estimate of the overall value of the Data Market	64,820	73,754	81,940	11.1%

Fig.5 - Valore e crescita (%) del mercato complessivo dei dati (€M), 2021-2023 - Fonte: European Data Market Study 2021-2023

Riguardo ai singoli paesi membri dell’UE, nel 2023 la Germania possedeva la quota più grande del mercato europeo dei dati, con un valore all’incirca del 60% maggiore rispetto a quello della Francia che occupa il secondo posto. Le cinque principali economie europee (Germania, Francia, Italia, Paesi Bassi e Spagna) hanno registrato dal 2022 al 2023 una crescita di poco minore della media europea. La somma delle quote di questi cinque paesi corrisponde a più di due terzi del mercato dei dati nell’UE. Questo risultato è parzialmente riconducibile alla dimensione superiore delle loro economie e al fatto che possiedono una forte presenza in settori strategici legati ai dati, rafforzando le loro posizioni di leadership.

Quando si parla di acquisto e vendita di dati, ci si riferisce anche al concetto di *monetizzazione dei dati* che rappresenta “il fatturato che i fornitori di dati ottengono dalla vendita dei dati.”. Si tratta di un segmento in ascesa e ancora non del tutto visibile del mercato dei dati, concentrato sulla vendita di dati invece che di hardware, software o servizi. Tipicamente si tratta di dati sulla localizzazione che permettono di ottenere informazioni sulla posizione di oggetti e persone, dati sugli acquisti in modo tale da comprendere le preferenze delle persone e dati riguardanti le performance di attrezzature, macchinari o equipaggiamenti. In confronto al 2022, la monetizzazione dei dati è aumentata del 20,6% nel 2023 con un valore di 25,4 miliardi, anche se risulta inferiore alla crescita del 28,3% del 2022 paragonata al 2021.

Legata al mercato dei dati, è presente l’*economia dei dati* che calcola gli effetti globali del mercato dei dati sull’economia. Al suo interno sono incluse la generazione, la raccolta, l’archiviazione, l’elaborazione, la distribuzione, l’analisi, la consegna e l’utilizzo dei dati abilitati dalle tecnologie

digitali. L'economia dei dati va oltre il semplice mercato in quanto tiene in considerazione valore e benessere prodotti dall'uso di essi nell'intero ambito economico, non limitandosi alle sole imprese.

Sono presenti tre categorie di impatti nell'economia dei dati: i ricavi generati dalle imprese di dati vengono rappresentati come impatti diretti, indiretti e indotti:

- *Impatti diretti* – Si tratta di effetti iniziali e immediati prodotti dalle imprese che offrono dati. Questa tipologia di impatti di natura quantitativa riguarda i ricavi derivanti dalla vendita di prodotti e servizi basati su dati.
- *Impatti indiretti* – Corrispondono alle attività economiche prodotte dalle società che forniscono dati nel corso della supply chain di un'azienda, inclusi i fornitori di input e i clienti delle aziende che forniscono dati.
- *Impatti indotti* – riguarda l'attività economica prodotta come effetto secondario. La spesa supplementare indotta deriva sia dal salario dei nuovi lavoratori che dagli aumenti di stipendio di quelli esistenti. Questa stimola la generazione di nuove entrate nella quasi totalità dei settori dell'economia. Invece, il consumo addizionale sosterrà l'attività economica di diversi settori come beni di consumo e vendita al dettaglio.

Nel 2022, l'economia europea dei dati è arrivata ad un valore di 500 miliardi, mentre nel 2023 ha oltrepassato i 544 miliardi di euro registrando un incremento annuale del 9,3%. A dispetto delle recenti sfide economiche, il mercato delle tecnologie dei dati e dell'intelligent analytics è stato quello maggiormente dinamico. Le imprese stanno comprendendo in misura sempre maggiore la rilevanza di un migliore uso dei dati per ottenere vantaggi competitivi e trasformare la propria impresa. La diminuzione della crescita del mercato di data analytics causata dalle recenti turbolenze economiche e politiche non è stata di lunga durata. Da una parte, i dati sono stati accettati come il motore per un progresso incessante, mentre dall'altra parte aumenta il riconoscimento della rilevanza della modalità con la quale i dati sono sfruttati come dimostra l'Artificial Intelligence Act, il cui obiettivo è quello di “regolamentare lo sviluppo e l'uso dell'intelligenza artificiale in Europa”.

Da una prospettiva tecnologica, il mercato ICT ha conseguito buoni risultati nel 2023, conformemente alle previsioni, grazie alla crescita a doppia cifra del mercato del software e alla transizione verso il cloud. L'adozione di sistemi di AI Generativa ha segnato il 2022, stimolando interesse tra utenti e providers favorendo un'analisi maggiormente dettagliata su regolamentazione, uso ed etica dei dati.

N.							Growth Rate 2022–2023	Impact on GDP, 2021	Impact on GDP, 2022	Impact on GDP, 2023
5.1 5.2	EU27	Value of the data economy and impacts on EU GDP	Value of total impacts on the EU economy and % of EU GDP	455,672	497,806	544,101	9.3%	3.7%	3.9%	4.2%
5.1 5.2	EU27+UK	Value of the data economy and impacts on EU GDP	Value of total impacts on the EU economy and % of EU GDP	593,846	650,418	709,570	9.1%	4.1%	4.3%	4.7%
5.1 5.2	Total, all countries	Value of the data economy and impacts on EU GDP	Value of total impacts on the EU economy and % of EU GDP	645,987	706,512	770,184	9.0%	4.1%	4.24%	4.7%

Fig.6 – Data Economy, 2021-2023: valore (milioni di €), crescita (%) e impatto sul PIL (%) –
Fonte: European Data Market Study 2021-2023

2.6 Data Marketplace

La recente comparsa dei *data marketplace* ha offerto una possibilità per superare il contrasto tra la tutela dei diritti individuali e l'incoraggiamento dell'interesse collettivo, che costituisce la sfida principale nelle moderne tecnologie che fanno un uso intensivo dei dati. L'obiettivo dei data marketplace è quello di sfruttare la monetizzazione dei dati per bilanciare la privazione della privacy delle persone e l'uso di dati privati. Su un versante del mercato, ci sono i detentori di dati (persone o imprese) che possiedono i propri dati personali e sono disposti a cederli in cambio di una retribuzione economica che dovrebbe rispecchiare la compromissione della privacy dovuta alla condivisione. Mentre nell'altro versante sono presenti i consumatori di dati come pubblicitari, operatori di servizi, rivenditori e produttori i quali desiderano i dati privati per finalità analitiche a tal punto da essere disponibili a pagare sulla base del valore economico prodotto. Un data marketplace rappresenta un ambiente digitale nel quale proprietari e consumatori di dati entrano in contatto ed effettuano l'acquisto e la vendita di dati in maniera agevole. In diversi casi, un broker di dati agirebbe come intermediario tra proprietari e consumatori, occupandosi di collezionare, combinare, memorizzare, ridistribuire e produrre ricavi da queste attività. Il broker potrebbe rappresentare una parte integrante della piattaforma oppure un attore esterno.

I Data marketplace variano a seconda della loro struttura e si possono identificare tre tipologie: *sell-side*, *buy-side* e *two-sided*. In un mercato del tipo *sell-side*, i dati sono raccolti da diverse fonti per essere venduti ai consumatori. Mentre nella tipologia *buy-side*, persone e imprese possono monetizzare i loro dati, dando la possibilità ai broker di ottenere dati dai rispettivi proprietari. Infine, il mercato *two-sided* unisce entrambe le parti, permettendo ai detentori dei dati di offrire i propri dati ai consumatori. Dalla parte *sell-side*, il valore economico dei dati dipende dal valore aggiunto che i consumatori prevedono di ottenere da essi, mentre nella parte *buy-side*, il valore dei dati riflette la quantità di privacy a cui rinuncia il proprietario come conseguenza dello scambio. Nel momento in cui due controparti sono connesse tramite un broker, il prezzo dei dati dovrebbe riflettere le valutazioni di consumatori e proprietari. Riguardo a questi ultimi, quelli che hanno minori necessità di privacy, dovrebbero ricevere una retribuzione più elevata, mentre i consumatori con esigenze informative maggiori dovrebbero sostenere costi maggiori.

Nonostante il concetto di scambio di prodotti digitali fosse già stato esaminato nel 1998 in un lavoro di Armstrong e Durfee, l'espressione "data marketplace" venne ideata nel 2013 da Schomm, Vossen e Stahl quando descrissero il data marketplace come una piattaforma nella quale gli utenti comprano varie licenze per avere accesso a diversi set di dati. In seguito, Vossen, Stahl, Löser e Muschalle affermarono che oltre a facilitare l'incontro tra domanda e offerta, i data marketplace giocano un ruolo fondamentale nella raccolta, nella memorizzazione e nell'armonizzazione del formato dei dati. In tempi più recenti, Stahl e Vossen hanno ampliato lo scopo dei data marketplace con la compravendita di qualunque servizio legato ai dati invece che la semplice compravendita di set di dati.

Essenzialmente le categorie di attori coinvolti sono tre: proprietario, consumatore e broker dei dati. I *proprietari* detengono i dati e desiderano trarne profitto, come nel caso di persone che dispongono di dati di tipo sociale, geografico, sanitario o finanziario oppure nel caso di imprese che acquisiscono dati sui loro clienti. I *consumatori* hanno come obiettivo quello di sfruttare i dati esterni per

ottimizzare le loro decisioni, lo sviluppo dei prodotti, le relazioni con i clienti e i servizi. Alcuni esempi sono “inserzionisti, sviluppatori di software, rivenditori, produttori, fornitori di servizi di telecomunicazione”. Infine, i *broker* che rappresentano dei mediatori i quali acquisiscono dati dai proprietari e li combinano con i dati aperti per poi venderli ai consumatori, ottenendo profitto.

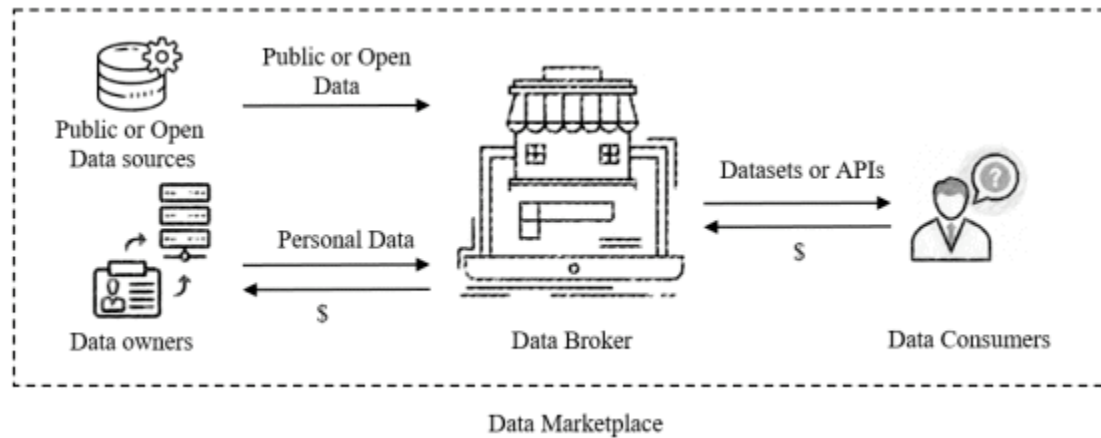


Fig.7 – Business model di un Data Marketplace – Fonte: A Survey of Data Pricing for Data Marketplaces

Seppure le operazioni di un broker di dati comprendano l’acquisizione e la vendita di dati, il loro core business può cambiare a seconda del tipo di data marketplace. In base al volume di transazioni bilaterali che avvengono in uno scambio di dati, la struttura viene definita nei seguenti modi:

- *Mercato one-sided*: si focalizza esclusivamente sul lato acquirente (buy-side) o quello venditore (sell-side).
 - *Mercato buy-side*: il broker ottiene dati da vari proprietari di dati e li remunera. Questa tipologia è destinata ad aziende e persone che desiderano trarre un profitto dai loro dati.
 - *Mercato sell-side*: le figure coinvolte sono i broker e i consumatori, i quali rappresentano imprese e individui alla ricerca di sorgenti esterne di dati per scopi analitici.

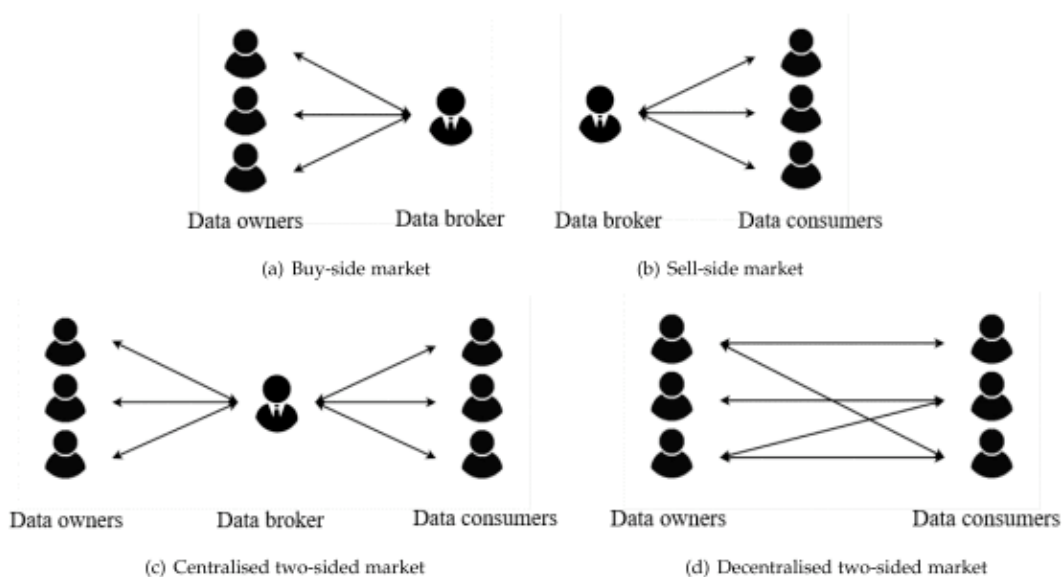


Fig.8 – Quattro strutture di Data Market – Fonte: A Survey of Data Pricing for Data Marketplaces

- *Mercato two-sided*: il broker di dati mette a disposizione una piattaforma di trading di dati per proprietari e consumatori ed ottiene un ritorno economico per ogni transazione.
 - *Mercato two-sided centralizzato*: il broker sarà responsabile della determinazione dei prezzi di acquisto per i proprietari e dei prezzi di vendita per i consumatori. Il beneficio economico del broker deriva dalla differenza tra i ricavi conseguiti con la vendita e le spese sostenute per l'acquisizione dei dati. Un esempio concreto è la Data & Sons che nel ruolo di intermediario di dati, “monetizza i dati personali dei proprietari di dati e vende informazioni aggregate ai consumatori di dati”.
 - *Mercato two-sided decentralizzato*: Il broker mette semplicemente una piattaforma di trading a disposizione di proprietari e consumatori, senza essere preso in causa nelle transazioni, le quali avvengono tra i membri della suddetta piattaforma.

2.7 Valorizzazione dei dati

Nel 2020, i ricercatori A. Galiano, A. Leogrande, S. Massari e A. Massaro hanno pubblicato un lavoro che “pone l’attenzione sui dati non personali ovvero quelli generati nell’ambito dell’Internet of Things - IoT nel settore pubblico e privato” e la cui finalità è relativa “all’indagine della natura di tali dati e delle ragioni giuridiche della loro tutela nonché all’esame di modelli economici e di mercato di valorizzazione degli stessi.”

Le informazioni che si possono ricavare dai dati sono in grado di avere una rilevanza pubblica o collettiva, non soltanto per il potenziale valore interpretativo che potrebbe offrire ai responsabili delle politiche pubbliche, ma anche per la sua condivisione o accessibilità che potrebbe incrementare la qualità delle analisi delle dinamiche economiche e sociali affrontate da ciascun ente sia pubblico che privato, migliorando in questo modo la capacità di valutazione e comprensione di un sistema. Di conseguenza, ciò ha indotto a fare riferimento alla *knowledge society*, all’interno della quale i dati rappresentano la risorsa essenziale per guidare le scelte dei responsabili pubblici e degli attori del mercato, contribuendo così a potenziare la competitività, i servizi resi e le performance economiche delle attività industriali e finanziarie, oltre che le applicazioni con impatti sociali positivi. È importante riconoscere il potenziale dei dati di creare valore come un elemento caratteristico della *knowledge society* attraverso l’equazione seguente:

$$KnowledgeSociety = f(CapitaleUmano; Informazioni; Tecnologia)$$

Allo stesso tempo, il dato pare acquisire il valore di commodity, come semplice bene di scambio economico.

Si possono individuare 3 potenziali prospettive riguardanti la relazione e la gestione del dato:

- Impiego strategico del dato, escludendo l’accesso a terzi e mantenendo in modo esclusivo l’informazione ottenibile, relativa unicamente al proprio set di dati;
- Conversione del dato in valore economico tramite la vendita;
- Inserimento del dato in un flusso globale e omnicomprensivo in grado di accumulare il massimo quantitativo di informazioni, allo scopo di agevolare processi di apprendimento e valutazioni di un fenomeno descrivibile in maniera quanto più approfondita e condivisa.

Riguardo alla sua natura, il dato può essere non-rivale, ovvero se un soggetto lo usa non impedisce ad un altro di utilizzarlo allo stesso tempo in maniera profittevole perché l’uso non consuma né la funzione né il dato stesso, fatta eccezione per l’inevitabile obsolescenza. Questo elemento definisce il dato con una connotazione tipica della dimensione del public good, ovvero non rivale e non-escludibile. I poli opposti corrispondono al bene pubblico e al bene privato (rivale e escludibile), ma possono esistere delle categorie intermedie. I common-pool good sono beni non escludibili perché non si può impedire a qualcuno di appropriarsi di essi, ma allo stesso tempo la loro quantità è limitata e chi li prende li esclude dalla disponibilità degli altri rendendoli beni rivali. Invece, i beni escludibili e non rivali prendono il nome di beni di club perché l’impiego del bene è limitato a un gruppo specifico di individui autorizzato all’uso. Ciononostante, l’utilizzo da parte di un soggetto non consuma il bene, di cui potrà usufruire un altro membro del club.

I dati sono oggetto di una stima economica al fine di stabilire valore e prezzo. Il tema risulta particolarmente delicato perché la determinazione del prezzo è un fattore cruciale e complesso da risolvere, in quanto condizionato da variabili in continua evoluzione e da una rilevante componente soggettiva legata all'intenzione di una parte di acquisire tali dati, col fine di migliorare i suoi processi produttivi o le attività di marketing ad esempio. Quindi il legame tra valore e prezzo rappresenta un aspetto cruciale nel processo di data monetization:

$$DataValorization = f(Value; Price)$$

All'interno dell'articolo, la *valorizzazione dei dati* viene espressa come “la capacità di ottenere un prezzo di mercato in grado di riflettere il valore dei dati”. L'uguaglianza tra valore e prezzo rappresenta l'ottimo del processo di valorizzazione dei dati, però si verifica nel lungo periodo esclusivamente in presenza di un mercato perfetto mentre l'evoluzione tipica dei mercati è segnata dalla disuguaglianza tra valore e prezzo. Per stabilire il *valore dei dati*, si può prendere in considerazione il legame tra valore intrinseco, valore estrinseco e valore di scambio.

$$DataValue = f(InnerValue; ExtrinsicValue; ExchangeValue)$$

Il *valore intrinseco* incide sui fattori presenti nei dati ed è legato positivamente al volume di dati preso in considerazione: all'aumentare della quantità di dati considerati, cresce il possibile valore interno del set di dati perché incrementa l'abilità sia descrittiva che quella di fornire informazioni approfondite. Il valore intrinseco riguarda le informazioni specifiche contenute nei dati, oltre a determinare la loro natura e presupporre una consapevolezza della controparte interessata alle caratteristiche dei dati.

Il *valore estrinseco* rappresenta il valore che l'acquirente assegna ai dati in base alle aspettative di beneficio derivanti dal loro utilizzo. Queste ultime derivano dal marketing che il venditore potrebbe svolgere sui dati e dalla credibilità dei dati.

Il *valore di scambio* nasce dal legame tra domanda e offerta all'interno di un mercato strutturato. Tale valore si realizza tenendo in considerazione l'eventualità di trasferire i dati sul mercato secondario. Il fatto che esista un valore di scambio segnala un avanzamento notevole del mercato dei dati.

Per quanto riguarda il *prezzo*, viene proposto un modello fondato su 3 fattori:

- Scarsità
- Usabilità
- Escludibilità

$$DataPrice = f(Scarsità; Usabilità; Escludibilità)$$

La *scarsità* può derivare dalle peculiarità del bene o del mercato e rappresenta uno scenario di mercato relativo alle merci. Inoltre, può essere causata dalle circostanze nelle quali si trovano alcuni player del mercato (acquirenti, consumatori o fornitori) oppure dalla struttura del mercato. Il fatto che le transazioni siano limitate rappresenta un esempio di scarsità dovuto alla struttura del mercato. Infine, i prezzi aumentano al crescere della scarsità.

L'*usabilità* rappresenta l'abilità dei dati nel creare valore per gli acquirenti e produrre profitti per i fornitori tramite la loro capacità di fornire informazioni accurate e rilevanti. Il prezzo è positivamente correlato all'*usabilità*, la quale è legata agli aspetti naturali dei dati come singolarità, celerità nel rilascio del dato sul mercato o innovatività e alla competenza del venditore di trasformare i dati in informazioni utili per il cliente. Concludendo, il mercato secondario può essere sviluppato sfruttando l'*usabilità*.

Con l'*escludibilità*, si indica la volontà dell'acquirente di impedire l'uso dei dati da parte di altri. La capacità di esclusione rappresenta un aspetto fondamentale dei diritti di proprietà; infatti, i beni privati sono protetti dall'uso non autorizzato di terzi, tuttavia si dibatte ancora sulla possibilità di poter applicare il concetto classico di proprietà anche ai dati.

La struttura del mercato può incidere su DataValorization, DataValue e DataPrice, determinando un prezzo in grado di rispecchiare il valore delle informazioni derivabili dai dati.

L'aspetto fondamentale per capire il valore dei dati consiste nella loro abilità ad aumentare il loro valore grazie a "circolazione, interpretazione e funzionalizzazione dei dati.". Anche se il dato possiede un valore intrinseco, acquisisce una valutazione di mercato grazie alla sua abilità di inserirsi nella dinamica di domanda e offerta; in altre parole, grazie alla presenza di soggetti disposti a pagare per ottenere i dati e di altri soggetti interessati a venderli in cambio di un compenso. Una volta che i dati vengono introdotti nella dinamica di domanda e offerta, il valore estrinseco del dato si manifesta. Nonostante ciò, il valore di scambio viene determinato dall'abilità del dato di essere oggetto di una vendita a scopo speculativo; vale a dire che l'acquirente fissa un prezzo che può far parte di una funzione di produzione. Dopo aver pagato il prezzo, quest'ultimo ottiene il dato che potrà vendere ad altri clienti come nel caso di una relazione B2B oppure creare una dimensione produttiva che consiste nell'inserimento del dato nella struttura organizzativa aziendale in previsione di un dipartimento del tipo data science in collegamento con la divisione marketing con lo scopo di aumentare servizi e produzione. In conclusione, il valore di scambio esiste esclusivamente in caso di monetizzazione dei dati e integrazione nella funzione produttiva dell'acquirente.

Nell'ottica di considerare il dato come un bene privato, ci sarebbero importanti conseguenze su prezzo, valore e valorizzazione. Si tratta di una tipologia di bene che si distingue per l'esclusione dall'uso collettivo e per essere limitato ad un rapporto esclusivo con un unico proprietario o pochi soggetti autorizzati all'uso. In questo modo, il prezzo subisce un effetto positivo tramite l'incremento del valore del fattore scarsità. D'altra parte, il valore subisce un'influenza negativa perché il fattore valore intrinseco cresce con l'incrementare della quantità di dati che si riescono a unire. Anche il valore estrinseco diminuisce perché la fiducia nei confronti di un set di dati esiguo è minore. Allo stesso modo, l'esclusività influisce negativamente sull'*usabilità*. Concludendo, la funzione di valorizzazione perde fattori di valore nel caso di dato come bene privato.

Il caso opposto è quello del dato inteso come bene pubblico. La diffusione dei dati favorisce la massimizzazione della funzione di valorizzazione tramite l'aumento delle abilità descrittive e le informazioni estraibili. Altri benefici risiedono nella rimozione dei free riders che puntano semplicemente alla speculazione basata sulla vendita ad un prezzo superiore a quello di acquisto e nell'incremento degli operatori capaci di conferire valore ai dati tramite la distribuzione

dell'elaborazione dei dati. Oltre a garantire ai dati la massima circolazione, la diffusione in uno spazio collaborativo, consente agli operatori di accedere a svariate elaborazioni e interpretazioni derivanti dai dati.

In un tale contesto si possono identificare le seguenti categorie di mercato:

- *Mercati cooperativi* – I partecipanti possono adottare una strategia cooperativa per le attività di produzione, collezione e scambio di dati. Questi mercati possono essere di tipo orizzontale (player del medesimo settore) e verticale (player di una catena produttiva e di distribuzione). Le aziende di un medesimo settore possono unire le forze nello scambio dei dati al fine di incrementare la market share, mentre quelle all'interno della filiera possono ottimizzare la comprensione complessiva del sistema produttivo e distributivo, usando le informazioni ottenute dal sistema nel suo insieme per adattare i propri processi o intervenendo in maniera simultanea su quello globale.
- *Mercati competitivi* – Essi generano incentivi monetari per clienti e fornitori. Questi ultimi partecipano a mercati di questo tipo per accrescere i profitti, mentre i clienti vi si rivolgono per ottimizzare il livello di soddisfazione rispettando vincoli di budget. Questa tipologia di mercato ha il potenziale per espandere l'economia dei dati, ma può fallire. Come se non bastasse, possono dare origine ad esternalità negative, le quali si manifesterebbero in abusi di posizione dominante riguardanti gestione o conservazione dei dati. Al fine di poter diminuire la probabilità di accadimento di fallimenti di mercato, risulta fondamentale l'implementazione di regolamenti, autorità di controllo e politiche volte a limitare l'instabilità e le situazioni di crisi. Questa rappresenta in parte la direzione della strategia europea sui dati.
- *Sharing economy* – Si tratta di piattaforme nelle quali vengono inseriti dati che possono essere condivisi per promuovere l'accesso piuttosto che la proprietà.
- *Club* – Riferito esclusivamente ai fornitori, rappresenta un'organizzazione formale o non, incentrata sulla condivisione dei dati. I membri possono migliorare le performance reciproche e mettere a disposizione un vantaggio competitivo.

Capitolo 3-Normative

3.1 Inizi e contesto

L'Unione Europea si è posta come obiettivo quello di sviluppare un mercato unico dei dati che assicuri "la competitività globale e la sovranità dei dati dell'Europa". In questo modo nasceranno spazi condivisi a livello europeo per facilitare l'accesso a una maggiore quantità di dati per essere utilizzati in ambito economico e sociale, ma al tempo stesso preservando il controllo di imprese e persone che li producono. A tal fine risulta fondamentale "adottare misure legislative in materia di governance, accesso e riutilizzo dei dati".

Normalmente, le strutture giuridiche fondamentali per la nascita di un mercato sono il contratto e la proprietà. Quest'ultima stabilisce diritti su risorse limitate, mentre il contratto permette ai contraenti di trasferire questi diritti. Il problema risiede nel fatto che i dati non si adattano bene a questi precedenti concetti. In primis perché sono beni non esclusivi e quindi gli individui li possono condividere e commercializzare senza compromettere la possibilità di accedervi, potendo banalmente duplicarli. Inoltre, un problema correlato consiste nel fatto che non esiste un insieme unificato di normative che definisca i diritti sui dati. Questi ultimi non possono essere considerati come proprietà in quanto non sono beni tangibili e non sono solitamente protetti dalla norma riguardante la proprietà intellettuale, poiché mancano di originalità. In realtà, i diritti sui dati sono stabiliti attraverso un insieme composto da norme sulla tutela di essi, regolamenti di settore che riguardano aspetti come la diffusione di dati custoditi dalle istituzioni pubbliche e l'autoregolamentazione privata attraverso il diritto contrattuale.

Inizialmente, ricercatori e funzionari governativi a livello globale suggerirono la creazione di diritti di proprietà intellettuale su dati e set di dati. Questi diritti assomigliano alla proprietà in quanto consentono di escludere l'utilizzo da parte di altri individui su prodotti della creatività umana (invenzioni), per un periodo limitato. Tali diritti sono stabiliti dalla legge e, attualmente sono regolamentati da autorità giuridiche internazionali, nazionali e regionali. In base a questa logica, l'Unione Europea ha adottato nel 1996 la direttiva sui database al fine di introdurre una forma di tutela riguardante il copyright sui dati elettronici con l'obiettivo di stimolare la creazione di database elettronici. In sostanza, la tutela della proprietà intellettuale sui dati avviene in situazioni molto specifiche all'interno delle quali i dati rappresentano espressioni della creatività umana e non quando sono generati da apparecchi digitali, come accade nella maggioranza delle situazioni. Effettivamente, la norma riguardante la proprietà intellettuale si basa sul concetto che i produttori sono incentivati a investire nell'innovazione quando ottengono un ritorno appropriato, tuttavia questo incentivo viene meno nel momento in cui i produttori non riescono a trattenere una parte rilevante del valore della loro innovazione nel caso in cui altri possono replicarla agevolmente.

In uno dei pochi lavori di ricerca condotti a livello europeo sull'economia dei dati, Nestor Duch-Brown et. al. mettono in evidenza che esistono differenze significative nelle finalità politiche che supportano i diritti di proprietà intellettuale e nelle modalità con le quali i dati vengono generati a livello globale. Queste differenze sembrano giustificare la restrizione nello sviluppare diritti analoghi sulla proprietà dei dati. Innanzitutto, non risulta così evidente se i diritti di proprietà siano essenziali per la loro generazione in quanto i dati rappresentano frequentemente un prodotto secondario di

attività commerciali già proficue e quindi la loro produzione non necessita di ulteriori incentivi. In aggiunta, i dati possono diventare con maggiore facilità escludibili grazie a misure di protezione tecnica rispetto alle invenzioni protette da copyright che sono destinate ad una diffusione su larga scala. Infine, il valore dei dati è sovente legato alla loro tempestività e ciò che assume maggior valore sono le informazioni che si possono estrarre con l'analisi e relazionando dati differenti tra loro. Duch-Brown et. al. concludono che l'idea del diritto di proprietà intellettuale in base alla quale la generazione di informazioni necessita di uno stimolo economico, non si applica ai dati. Di conseguenza, l'ipotesi secondo la quale per ottimizzare il benessere collettivo sia necessario assegnare diritti esclusivi ai dati potrebbe risultare priva di validità.

Anche se i dati non sono protetti da normative su proprietà o proprietà intellettuale, questo non implica che non esistano diritti legali su di essi. Per citare un caso concreto, secondo il GDPR, i dati prodotti da parte degli interessati, si possono utilizzare esclusivamente per motivazioni circoscritte, in modo particolare nel caso in cui l'interessato abbia dato il proprio consenso al trattamento dei dati. In aggiunta, il GDPR assicura agli interessati sia il diritto di richiedere la cancellazione di questi ultimi quando lo si desidera, sia il diritto alla portabilità dei dati, che permette il trasferimento dei dati da una piattaforma o sistema ad un altro senza restrizioni, aumentandone la supervisione da parte degli utenti.

Numerose ricerche, soprattutto negli Stati Uniti, hanno messo in luce l'importanza dell'ordinamento privato nel definire l'accesso e l'utilizzo dei dati. Julie Cohen e Amy Kapczynsky esperti di diritto, hanno sottolineato come l'ordinamento privato del mercato dei dati contribuisce a creare uno scenario di forte disuguaglianza negli Stati Uniti, nel quale utenti e altri stakeholder hanno un potere limitato e si assumono la responsabilità delle loro decisioni e dei metodi di trattamento dei dati. Le imprese tecnologiche che gestiscono grandi volumi di essi usano contratti di accesso e accordi di riservatezza per offrire alle imprese una licenza limitata nel tempo e riservata per sfruttare i dati a loro disposizione. Inclusi in questi contratti, sono presenti clausole che vietano la condivisione con terze parti, creando una situazione di apparente esclusività ed in questo modo, il controllo sull'uso di tali dati rimane nelle mani dell'azienda tecnologica che li ha originariamente generati o raccolti, come se ne avessero pieno possesso. Dopo aver analizzato questi fenomeni, Cohen e Kapczynski sono giunti alla conclusione che se consideriamo come scopo principale dei diritti di proprietà quello di definire chi può accedere ai beni e chi ha il controllo su di essi, in pratica sono presenti diritti sui dati che assomigliano alla proprietà. In aggiunta, visto che le principali aziende tecnologiche possiedono la gran parte dei dati e hanno il potere di stabilire chi possa accedervi, i mercati risultano estremamente sbilanciati a vantaggio dei principali possessori.

Come spiegato in precedenza, il diritto e l'economia classici affermano che il benessere si raggiunge più efficacemente promuovendo lo sviluppo dei mercati e questo si realizza attraverso l'istituzione di diritti di proprietà sulle risorse per evitare la 'tragedia dei beni comuni'. Quest'ultima rappresenta una situazione nella quale un eccesso di individui sfrutta una risorsa senza considerare i costi necessari e gli interventi di manutenzione o rigenerazione, determinandone il suo logoramento.

In maniera contrapposta, sono presenti delle ricerche riguardo alla governance dei beni comuni che argomentano l'esistenza di una soluzione alternativa. Elinor Ostrom, ha illustrato uno scenario nel

quale le comunità sono in grado di controllare efficacemente le risorse collettive se vengono seguiti otto principi famosi. Tra questi sono compresi:

1. la determinazione di confini di gruppo ben definiti;
2. l'istituzione di norme che regolano l'utilizzo dei beni comuni sulla base delle necessità e delle circostanze locali;
3. meccanismi partecipativi per modificare queste norme in modo tale che le risorse siano controllate con efficacia dalla comunità.

Yochai Benkler ha evidenziato che in presenza di confini non ben delineati come per i beni comuni ad accesso aperto, questi ultimi sono diffusi e prosperi nell'ambiente digitale connesso. Casi di applicazioni basate sui beni comuni che hanno generato un notevole valore comprendono software open source, le pubblicazioni open access e Wikipedia.

In accordo con ricerche analoghe, Brett Frischman ha dimostrato come i beni comuni ad accesso aperto e non, siano onnipresenti nelle economie moderne sotto l'aspetto di 'infrastrutture'. Frischman descrive le infrastrutture come risorse che producono valore se utilizzate come input in una varietà più ampia di processi produttivi. Inoltre, gli output di questi processi sono solitamente beni pubblici e non di mercato che producono esternalità positive, le quali avvantaggiano la società. Infine, gestire le risorse infrastrutturali in maniera liberamente accessibile può essere socialmente auspicabile quando semplifica queste attività a valle.

Studiosi e responsabili delle politiche pubbliche hanno utilizzato le precedenti considerazioni per proporre una gestione dei dati simili ai beni comuni o alle infrastrutture, piuttosto che come beni privati. Questa nuova visione risulta già presente nel rapporto "Data-Driven Innovation: Big Data for Growth and Well-Being" rilasciato nel 2015 dall'OCSE, nel quale i dati sono definiti come un bene accessibile a tutti e che dovrebbe essere normato in maniera più appropriata come un bene comune aperto. Una problematica relativa ai dati aperti riguarda il contrasto con interessi già consolidati come i diritti alla privacy. Questi conflitti diventano più evidenti con l'incrementare della disponibilità e della possibilità di risalire a singoli individui. Pertanto, pubblicazioni recenti hanno provato a bilanciare i vantaggi dei contesti di dati aperti con i rischi per la privacy e altri diritti ed interessi. Nel rapporto dell'OCSE (Organizzazione per la Cooperazione e lo Sviluppo Economico) del 2022 "Responding to Societal Challenges with Data", si sostiene che "l'accesso, la condivisione e il riutilizzo dei dati (apertura dei dati) possono generare significativi benefici sociali ed economici. (...) Tuttavia, l'apertura dei dati comporta anche dei rischi per individui e organizzazioni. Questi includono rischi per la privacy e la protezione dei dati, i diritti di proprietà intellettuale e la sicurezza digitale e nazionale". In particolare, al suo interno vengono suggerite soluzioni tecniche, organizzative e legali per equilibrare questi interessi e generare stimoli ed opportunità che consentano alle diverse parti di condividere i dati e sbloccare il loro valore, garantendo però la sicurezza.

3.2 GDPR

I dati raccolti da registratori di dati di evento e scatole nere assicurative comprendono dati personali noti come ‘Richiesta di accesso del soggetto’ oppure incidentalmente dati personali e non di terzi. Il concetto di ‘accesso accidentale’ è relativo al caso in cui il richiedente vuole ottenere un set di dati personali che sono strettamente collegati a quelli di altre persone. In tali circostanze, si attivano meccanismi di protezione contrapposti, per assicurare i diritti delle parti interessate, compresi i diritti di tutela dei soggetti i cui dati sono collegati. Nonostante ciò, l’accesso potrebbe essere autorizzato, se dopo un’attenta valutazione dei diritti in gioco, risulta giustificato.

Al momento, i diritti di accesso delle case automobilistiche sono circoscritti ai dati EDR, invece l’accesso per gli enti assicurativi è ristretto ai dati delle scatole nere ed il motivo risiede nel fatto che possono essere entrambi presenti all’interno di un veicolo ma non sono interconnessi.

Con riferimento all’accesso ai dati aggregati, se questi sono stati anonimizzati, non sono più ritenuti personali e di conseguenza le persone possono accedervi senza infrangere le disposizioni del GDPR. Questa tipologia di dati rappresenta informazioni rilevanti quando esaminate in gruppo, solitamente per finalità statistiche o di prova. Per esempio, si potrebbero acquisire insiemi di dati EDR anonimizzati al fine di regolare il traffico o usarli per class action dei consumatori nei confronti di un’azienda automobilistica che produce auto con parti difettose.

Secondo il *punto 1f) dell’articolo 6*, il trattamento dei dati personali è ritenuto legittimo nel caso in cui risulti indispensabile ai legittimi interessi del titolare del trattamento oppure di un terzo, a condizione che questi interessi non predominano su diritti e libertà della persona interessata. I legittimi interessi di terze parti possono riguardare scenari nei quali un altro soggetto diverso dall’interessato o dal titolare del trattamento ha una motivazione giustificata per accedere ai dati personali. In queste circostanze, il titolare può godere di solide basi giuridiche per trattare i dati personali se indispensabile al fine di tutelare i legittimi interessi del terzo. Per fare un esempio, una persona può avere come legittimo interesse quello di avere accesso ai registri di guida relativi ad un altro individuo nel caso in cui stesse valutando di noleggiare la sua vettura, come i rivenditori quando offrono le loro auto ai guidatori Uber. In maniera simile, se una persona volesse ingaggiare un autista per un viaggio, potrebbe essere legittimato ad accedere ai dati personali relativi al conducente per verificare il suo stile di guida.

In base al *punto 2f) dell’articolo 9*, il trattamento dei dati potrebbe risultare indispensabile nelle occasioni in cui sia domandato al fine di avviare, esercitare o difendere un diritto in sede legale oppure se i tribunali agiscono nell’ambito delle loro funzioni giurisdizionali. L’ipotesi presentata riguarda una persona che in veste di titolare del trattamento inoltra una richiesta per accedere ai dati personali di un altro individuo all’interno di una black box, invocando un interesse legittimo come l’acquisizione di elementi probatori a sostegno di una causa di responsabilità civile. In particolare, tramite questi dati si potrebbe stabilire se il guidatore partecipa di un incidente abbia assunto alcol o droghe. In modo tale da aderire al principio di minimizzazione dei dati, il destinatario dovrebbe poter accedere esclusivamente alle informazioni necessarie per giungere a tale inferenza, limitata ai dati acquisiti entro un periodo di tempo accettabile dopo l’incidente. In aggiunta, in base alle norme

stabilite dall'*articolo 9*, le case automobilistiche, utilizzando i dati EDR, possono servire da tramite tra i loro clienti e i servizi di emergenza quando si verifica un sinistro.

Secondo il *punto 1 dell'articolo 15*, l'interessato è in possesso del diritto che gli consente di richiedere al titolare del trattamento, la verifica sul fatto che i suoi dati personali siano o meno oggetto di trattamento e qualora lo siano, ha il diritto di potervi accedere e di ottenere una copia. In termini generali, le normative sulla tutela dei dati riconoscono agli individui il diritto di accesso ai loro dati personali posseduti da un titolare del trattamento. Ad ogni modo, come già menzionato, esistono circostanze nelle quali una persona può chiedere di accedere ai suoi dati personali che incidentalmente coinvolgono anche un'altra persona. In tali situazioni, il titolare del trattamento deve verificare il rispetto di specifici requisiti, uno di questi è che le informazioni domandate debbano riferirsi anche all'interessato. Questo implica che l'interessato deve avere una motivazione giustificata per l'accesso, come nel caso in cui un individuo A consulta i propri dati per dimostrare che l'individuo B si trovava in auto con loro.

Nonostante le restrizioni sulle possibili attività di trattamento dei dati personali di terzi, un titolare del trattamento non può negare il diritto di accesso dell'interessato, anche nel caso in cui la sua richiesta si fondi su diritti successivi, come quello alla cancellazione.

Secondo l'*articolo 16*, l'interessato è in possesso del diritto di domandare che il titolare del trattamento corregga senza indugi ogni informazione personale errata. Inoltre, in base alle finalità del trattamento, ha il diritto di acquisire il completamento di eventuali informazioni personali mancanti che lo interessano, il che potrebbe implicare la consegna di ulteriori informazioni al titolare del trattamento. Nel momento in cui l'interessato presenta una richiesta di rettifica, le operazioni che riguardano i dati personali che spettano tanto all'interessato quanto ad un terzo si estendono maggiormente in confronto alla richiesta basilare di accesso. Anche se l'accesso ai dati è consentito, se si tratta di personali, parziali o non corretti, potrebbe essere necessario crearne di nuovi, aggiornarli o cancellarli.

Secondo l'*articolo 17* l'interessato possiede il diritto di domandare al titolare del trattamento l'eliminazione immediata dei suoi dati personali. Come disposto in seguito al caso Google Spagna, le persone hanno il diritto di esigere l'eliminazione dei loro dati personali quando questi ultimi risultano inesatti, inadeguati, non pertinenti o eccessivi rispetto agli scopi per la loro elaborazione. Il concetto 'inadeguati' può includere circostanze nelle quali i dati non siano più utili, il consenso sia stato revocato e non esistano altre basi legali per l'elaborazione, l'elaborazione sia illegittima oppure siano state presentate obiezioni fondate.

L'obiettivo fondamentale dell'*articolo 20*, che tratta il diritto alla portabilità, è quello di fornire maggiore autorità ai consumatori di servizi digitali, evitando che rimangano vincolati ad un solo fornitore di servizi digitali (lock-in) ma anzi rendendo più semplice il passaggio ad un altro fornitore e permettendo di usufruire di diversi servizi di piattaforma rivali simultaneamente senza limitazioni (multi-homing). Tutto ciò è possibile perché gli individui possono ottenere i loro dati personali e li possono inoltrare ad un altro titolare del trattamento. Al fine di assicurare l'interoperabilità dei dati tra sistemi e servizi, il set di dati personali si deve poter scaricare in un formato strutturato, solitamente adottato e comprensibile da una macchina. Secondo gli esperti del settore, il diritto precedentemente

citato si può applicare ai dati relativi al veicolo. Se le condizioni lo permettono, l'individuo è in diritto di chiedere al titolare del trattamento iniziale, lo spostamento dei dati ad un altro titolare del trattamento. Nonostante ciò, la praticità di questo trasferimento dipende da specifici set di dati. Si possono verificare vincoli di tipo tecnico qualora lo spostamento diretto comprometta il funzionamento del servizio, mentre potrebbero emergere vincoli di natura economica se il soddisfacimento della richiesta risulti troppo oneroso per il titolare del trattamento.

In base all'*articolo 23*, si possono applicare delle limitazioni nei confronti dei diritti degli interessati o degli obblighi dei titolari del trattamento a patto che tali limitazioni non compromettano l'essenza dei diritti e delle libertà essenziali. Le limitazioni sono consentite esclusivamente nel caso in cui siano indispensabili e adeguate in un contesto democratico al fine di tutelare la sicurezza pubblica, difendere la vita delle persone, evitare o combattere crimini, applicare sanzioni penali, proteggere rilevanti interessi pubblici di uno stato o dell'intera Unione Europea, inclusi quelli economico finanziari, conservare registri pubblici, trattare ancora i dati personali conservati a fini precisi o tutelare l'interessato o i diritti e le libertà altrui.

All'interno del GDPR, sono previste delle deroghe specificate tra l'*articolo 85* e l'*articolo 89*. Tramite un fondamento giuridico solido, queste deroghe permettono ai titolari del trattamento di gestire i dati personali di un interessato in particolari situazioni. A titolo di esempio, queste ultime riguardano l'esercizio della libertà d'espressione e informazione a finalità giornalistiche, di ricerca oppure creative. In aggiunta, i dati personali presenti all'interno di documenti ufficiali di istituzioni pubbliche possono essere divulgati allo scopo di "conciliare l'accesso del pubblico ai documenti ufficiali e il diritto alla protezione dei dati personali ai sensi del presente regolamento".

Un altro aspetto importante da tenere in considerazione riguarda le deroghe previste nell'*articolo 89*, le quali possono essere utilizzate come vie di accesso in modo da consentire a terzi di superare la protezione dei dati personali, ma solo se vengono rispettate specifiche garanzie. Nello specifico l'*articolo 89* dispone che il trattamento di dati personali per fini di conservazione nell'interesse pubblico, per attività di ricerca scientifica o storica oppure per finalità statistiche debba avvenire in osservanza di garanzie appropriate. Queste ultime consistono in provvedimenti tecnici per rispettare il principio di minimizzazione dei dati, come l'adozione di tecniche di anonimizzazione.

Nel Febbraio del 2020, la Commissione europea ha rilasciato la strategia sui dati, la quale viene inserita nel quadro più generale della trasformazione digitale a livello economico e sociale, evidenziando la necessità di dare priorità agli interessi delle persone in un contesto come quello della società attuale, nella quale si producono volumi di dati in costante aumento. I regolamenti chiave che mettono in atto tale strategia sono il Data Governance Act e il Data Act.

3.3 Data Act

Il Data Act (DA) ha come obiettivo quello di potenziare l'accesso ai dati e conseguire una ripartizione più bilanciata dei vantaggi ottenuti attraverso l'uso e il riutilizzo dei dati. Diversamente dal Data Governance Act, il Data Act non prevede l'istituzione di enti per promuovere la condivisione di dati, bensì stabilisce degli obblighi vincolanti.

Il documento è suddiviso in undici capitoli, che delineano norme su vari aspetti, tra cui la condivisione di dati tra impresa e consumatore (Business to Consumer) e tra impresa e impresa (Business to Business o B2B), obblighi per i titolari di dati, clausole contrattuali inique, condivisione di dati tra impresa e governo (B2G) e interoperabilità.

In particolare, gli scopi sono:

1. agevolare accesso ed uso ad opera di consumatori e imprese, mantenendo allo stesso tempo gli incentivi per gli investimenti nella produzione di dati;
2. fornire alle istituzioni pubbliche la possibilità di accedere a dati aziendali in situazioni straordinarie;
3. stabilire degli standard di interoperabilità nel caso di dati da riutilizzare tra settori.

La parte introduttiva del regolamento comincia con l'individuazione delle barriere alla condivisione che non consentono una distribuzione ottimale dei dati a beneficio della società. Queste comprendono la carenza di incentivi a favore dei titolari per concludere spontaneamente contratti di condivisione dei dati, ambiguità riguardo a diritti e obblighi legati ai dati, i costi associati alla stipula di contratti e lo sfruttamento delle disparità contrattuali in relazione all'accesso e all'utilizzo. Il Data Act intende eliminare queste barriere mediante la definizione di un insieme coerente di regole che indichino "chi ha il diritto di utilizzare i dati di un prodotto o di un servizio correlato, a quali condizioni e su quale base". Di conseguenza, il fulcro del regolamento è rappresentato dalle disposizioni che stabiliscono diritti e obblighi per l'accesso.

L'*articolo 3* rappresenta la disposizione iniziale che impone ai titolari, i quali corrispondono tipicamente ai produttori, come le case automobilistiche che dotano le loro vetture di EDR, l'obbligo di consentire l'accesso da parte dell'utente ai dati di prodotti connessi e servizi correlati "in modo facile, sicuro, gratuito". Questo permette all'utente di trasmettere o condividere i dati con altre imprese, tra cui compagnie assicurative, altre case automobilistiche, studi legali, distributori di carburante e così via. Sempre i produttori hanno l'obbligo di fornire informazioni dettagliate, tra cui il volume di dati raccolti e le finalità per le quali vengono utilizzati. Il suddetto obbligo generalmente riguarda i requisiti tecnici e i piani di progettazione utilizzati per realizzare l'EDR. Il fatto che i dati debbano essere 'direttamente accessibili' appare come superiore all'equivalente presente nel GDPR che consiste in un semplice diritto di lettura; poichè non rientra in maniera esplicita nella classificazione CRUD (create, read, update, delete), suggerisce che il Data Act espande i diritti dell'individuo.

L'opposto del succitato obbligo corrisponde al diritto di accesso e uso per gli utenti relativamente ai dati di prodotti connessi e servizi correlati, sancito dall'*articolo 4*. Il principio su cui si basa questo

articolo è legato alla circostanza che la produzione dei dati deriva dall'interazione di perlomeno due attori, ovvero il progettista o il produttore di un prodotto connesso, il quale spesso funge anche da fornitore di servizi correlati, e l'utente del prodotto o del servizio correlato. Proprio per questo motivo viene riconosciuto agli utenti il diritto precedentemente citato, in quanto rappresentano una figura essenziale per la produzione dei dati. Questo diritto trova applicazione nel caso in cui i dati non siano fruibili in maniera diretta dall'utente tramite il prodotto connesso o il servizio correlato, come accade per ogni dato acquisito dall'EDR che non è visibile attraverso un'interfaccia. In queste situazioni, l'utente ha diritto ad accedere ai dati in modo rapido, senza costi, continuo e in tempo reale. In base al *punto 6 dell'articolo 4*, titolare e utente possono concordare delle strategie per tutelare la riservatezza dei dati scambiati, soprattutto rispetto a terzi. Questa misura fornisce un rimedio concreto al problema sollevato dall'articolo 20 del GDPR, disponendo che lo spostamento dei dati non deve compromettere i diritti dei terzi. Inoltre, facilita il trasferimento sicuro dei dati, persino quando sono coinvolte informazioni relative ad altri. Tale condizione può avvenire qualora i dati del sistema EDR includano informazioni relative a soggetti differenti dall'utente.

Un altro diritto a disposizione degli utenti riguarda la possibilità di condividere i dati con terze parti, il quale permette di espandere e arricchire il diritto alla portabilità definito nel GDPR. Nello specifico, l'*articolo 5* afferma che “Su richiesta di un utente, o di una parte che agisce per conto di un utente, il titolare dei dati mette a disposizione di terzi i dati prontamente disponibili, nonché i pertinenti metadati necessari a interpretare e utilizzare tali dati, senza indebito ritardo, con la stessa qualità di cui dispone il titolare dei dati, in modo facile, sicuro, a titolo gratuito per l'utente”. Proprio questa norma rafforza la posizione giuridica degli utenti riguardo all'accesso dei loro dati. Anche se i dati hanno uno scarso valore per gli utenti, non si può dire lo stesso riguardo alle micro, piccole e medie imprese che provano a fornire servizi post-vendita legati ai prodotti connessi come assistenza tecnica e manutenzione. In mancanza di questi dati, ogni azienda che tenta di contendere i servizi post-vendita con i produttori sarebbe in una posizione di svantaggio competitivo: l'accesso ai dati sulle performance permette ai produttori di proporre servizi migliori se confrontati con quelli di qualunque rivale. Il Data Act tenta di modificare questa circostanza permettendo “un'offerta competitiva di servizi post-vendita”.

Il terzo articolo interpretato in combinazione con il quinto assicura una trasmissione di dati senza ostacoli tra le imprese previa richiesta dell'utente EDR, in modo tale che le aziende possano scambiare i dati in maniera orizzontale con i diversi soggetti coinvolti.

L'implementazione di questa serie di diritti e obblighi è rilevante dalla prospettiva della tecnica di regolamentazione. I metodi normativi tradizionali per affrontare i fallimenti di mercato e organizzare i mercati comprendono le iniziative dell'antitrust, le normative di settore che agiscono sui parametri economici mediante, per esempio, norme per i prezzi o per le esternalità. Eppure, i fallimenti di mercato verso i quali è rivolto il Data Act non sono convenzionali ed in particolare riguardano il commercio inefficiente causato da una distribuzione vaga dei diritti. Dato che quest'ultimo rappresenta una delle questioni più intricate dell'economia dei dati, non stupisce che l'UE abbia optato per un approccio volto a “riassegnare i diritti per fornire maggiori incentivi al commercio”. Secondo quanto osservato da Zingales e Rolnik, questa scelta rappresenta la strategia più gradita da parte degli enti regolatori per agire in quei mercati che sono in via di sviluppo. Antecedentemente

all'introduzione del Data Act, l'economia dei dati non personali si fondava sulla 'regola di cattura': chiunque acquisisse dati, poteva detenerli e trarne ogni vantaggio derivante dal loro impiego e riutilizzo. Come conseguenza di ciò, la maggioranza dei dati in circolazione è in pratica posseduta dai principali attori del mercato, i quali godono della clientela e delle infrastrutture indispensabili per acquisire, conservare e analizzare enormi volumi di dati. Il regolamento afferma che "è preferibile adottare un approccio generale all'assegnazione dei diritti relativi all'accesso e all'uso dei dati" rispetto al sistema esistente nel quale le imprese che acquisiscono i dati beneficiano di "diritti esclusivi di accesso e uso", in particolar modo per la natura non rivale dei dati, che permette ad un numero indefinito di soggetti di beneficiare dei loro vantaggi. Se la redistribuzione dei diritti sarà una tattica vincente per ottenere i benefici economici sperati rappresenta una questione empirica che verrà chiarita dallo sviluppo in divenire dell'economia dei dati. A prescindere dal risultato effettivo, la strategia normativa adottata è innovativa; infatti, Rolnik e Zingales sostengono che essa rappresenta "una soluzione del XXI secolo per un problema del XXI secolo".

Vale la pena sottolineare che nel Data Act non sono i terzi ad avere il diritto di accesso ai dati, bensì gli utenti che hanno la possibilità di condividere con loro i dati. In effetti, il regolamento non prevede un effettivo sistema di condivisione B2B, semmai un modello ibrido 'B2C2B': pur essendo i dati trasferiti da impresa all'altra, è compito dell'utente iniziare il processo di trasferimento. Un meccanismo del genere solleva dubbi riguardo al fatto che sovrastimi la destrezza degli utenti nel gestire i loro dati e perciò potrebbe non riuscire nell'intento di ottimizzare la condivisione. Sebbene la presenza di diverse critiche riguardanti questo approccio dell'autogestione, presenti all'interno di opere riguardanti la governance dei dati, il Data Act si fonda su di esso, puntando sull'adozione di un sistema di incentivi che incoraggi gli utenti ad intraprendere processi di trasferimento di dati. Innanzitutto, la norma presenta un tema di dipendenza economica: domandare la condivisione dei dati favorisce una maggiore varietà di servizi post-vendita, il che implica che i consumatori non si affidino esclusivamente ai servizi offerti dal produttore. Successivamente, un movente di innovazione: potenziare l'accesso ai dati dei competitori stimola "una maggiore innovazione basata sui dati, oltre allo sviluppo di prodotti o servizi non correlati a quelli inizialmente acquistati o sottoscritti dall'utente". Questi due stimoli si fondano su una prospettiva moderna dell'economia, nella quale clienti e produttori sono posti in condizioni di uguaglianza e i clienti hanno il diritto di ricevere prodotti e servizi innovativi come riconoscimento per il loro contributo alla produzione di dati. Eppure, tutti e due questi riconoscimenti sono di lungo periodo e strutturali e ciò vuol dire che i clienti non ottengono vantaggi tempestivi e tangibili a fronte di costi di transazione necessari per avviare domande di condivisione. Questa decisione di progettazione potrebbe rappresentare una significativa restrizione all'efficacia della condivisione dei dati tra due imprese (B2B). Una possibile risposta sarebbe che le imprese individuino modalità per stimolare gli utenti ad inoltrare richieste di dati. Ad ogni modo, secondo il *punto 5 dell'articolo 5*, "Il terzo non utilizza mezzi coercitivi né abusa di lacune nell'infrastruttura tecnica di un titolare dei dati destinata a proteggere i dati al fine di ottenere l'accesso ai dati".

Oltre alla dipendenza degli utenti come mediatori, il sistema di condivisione B2B possiede altre restrizioni. In base al *punto 3 dell'articolo 5*, le aziende che offrono servizi di piattaforma di base e sono caratterizzate da un notevole potere economico (definite 'gatekeeper' nel Digital Market Act), non possono avvalersi del diritto in possesso da parte degli utenti riguardante la possibilità di

richiedere la condivisione dei loro dati. Tale restrizione è comprensibile, poiché si tratta di attori economici che sono già dotati di un accesso a enormi volumi di dati e il Data Act e la strategia europea dei dati tentano di affrontare i seguenti fallimenti di mercato: “le strozzature che impediscono l’accesso ai dati” e “squilibri nel potere di mercato”. Inoltre, il *punto 2e) dell’articolo 6* vieta a coloro che ricevono i dati di farne uso “per sviluppare un prodotto in concorrenza con il prodotto connesso da cui provengono i dati consultati né condivide i dati con un altro terzo a tal fine” e “per ottenere informazioni sulla situazione economica, sulle risorse e sui metodi di produzione del titolare dei dati o sull’utilizzo da parte di quest’ultimo”. Questa restrizione conferma la finalità del Data Act di “Facilitare l’accesso ai dati e il relativo utilizzo da parte dei consumatori e delle imprese, preservando nel contempo gli incentivi a investire in modalità di generazione del valore grazie ai dati”. Tuttavia, sorgono dubbi riguardo alla ragionevolezza di questa limitazione visto che una possibile conseguenza sarebbe quella di consolidare il potere di mercato in mano ai produttori, i quali non dovranno più preoccuparsi di una minaccia di entrata nel mercato da parte di rivali che offrono servizi post-vendita.

Riguardo ai segreti commerciali, il *punto 9 dell’articolo 5* stabilisce che debbano essere rivelati esclusivamente nel caso in cui siano indispensabili al fine di realizzare lo scopo stabilito tra utente e terzo e quest’ultimo è obbligato a mantenere la riservatezza sulle informazioni che riceve. Questo requisito rispecchia di nuovo la volontà del Data Act di trovare un equilibrio tra condivisione e accesso insieme ad altri interessi privati.

L’*articolo 7* stabilisce che le micro, le piccole e le medie imprese, sono esonerate dal dover condividere i dati dei loro utenti con terzi. Poiché risulta improbabile che le suddette imprese dispongano delle risorse tecniche necessarie al conseguimento di una condivisione con terzi agevole e senza problemi, costringerle a rispettare questi obblighi è ritenuto troppo gravoso. Questa scelta dimostra lo sforzo del regolamento per l’equità strutturale, che prevede un intervento positivo riferito all’imposizione di obblighi alle imprese che dispongono di elevati volumi di dati, oltre che un intervento negativo con riferimento all’evitare di sovraccaricare di spese i piccoli attori. Inoltre, sempre questa norma stabilisce i confini all’interno dei quali le case automobilistiche, i fornitori di polizze assicurative e le compagnie di assicurazione secondarie collaborano nella condivisione dei dati e di conseguenza agevola le pratiche di condivisione in capacità tanto verticali quanto orizzontali.

Il terzo capitolo del Data Act definisce gli obblighi che i titolari dei dati devono rispettare quando concedono l’accesso ai dati. In base al *punto 1 dell’articolo 8*, i dati devono essere messi a disposizione “a condizioni eque, ragionevoli e non discriminatori e in modo trasparente”. Successivamente, i titolari non possono concedere un trattamento privilegiato ai destinatari, soprattutto nel caso di aziende con le quali intrattengono relazioni commerciali e se il destinatario sia dell’idea che abbia subito discriminazione, sarà compito del titolare dimostrare il contrario. Il *punto 4 dell’articolo 8* afferma che il titolare non deve fornire i dati in maniera esclusiva ad un destinatario salvo che questa richiesta non venga espressamente esibita secondo le disposizioni del secondo capitolo del Data Act. Questo elemento risulta notevolmente vantaggioso per le imprese che offrono servizi di assicurazione per veicoli e permette agli interessati di spostare i loro dati da un titolare ad un altro. Tale semplicità di portabilità dei dati tra imprese ha un effetto positivo sulla competitività delle imprese, oltre che permettere ai loro clienti di ricavarne beneficio.

Proseguendo, l'*articolo 9* sostiene che i destinatari possono godere esclusivamente di un compenso che “è non discriminatorio e ragionevole e può includere un margine”. Qualora il destinatario corrisponda ad una PMI o un ente di ricerca che non persegue scopi di lucro, il compenso non deve eccedere i “costi sostenuti per mettere a disposizione i dati”.

Passando all'*articolo 10*, per risolvere potenziali controversie tra due parti bisogna usufruire degli organismi certificati da parte degli stati appartenenti all'unione europea.

Il quarto capitolo riguarda le clausole contrattuali illegittime tra imprese. Secondo l'*articolo 13*, le clausole contrattuali imposte da una sola parte ad un'altra controparte, risultano non vincolanti per quest'ultima se sono abusive, ovvero se “è di natura tale che il suo utilizzo si discosta considerevolmente dalle buone prassi commerciali in materia di accesso ai dati e relativo utilizzo, in contrasto con il principio di buona fede e correttezza.”

A differenza della condivisione B2B che poggia sul ruolo dell'utente come mediatore, *la condivisione tra impresa ed ente governativo (B2G)* si fonda sulla domanda da parte degli enti governativi: come stabilito nell'*articolo 14*, nel caso in cui un organismo pubblico provi l'esistenza di una ‘necessità eccezionale’ di usare i dati domandati, allora il titolare sarà obbligato a metterli a disposizione. Il fatto di dover dimostrare la presenza di un'esigenza fuori dall'ordinario, riduce notevolmente l'ambito di applicazione della condivisione B2G e probabilmente la ragione è dovuta all'intento di equilibrare gli interessi di attori privati e individui, come già detto in precedenza.

L'*articolo 15* presenta le seguenti ‘necessità eccezionali’:

1. emergenza pubblica;
2. dati la cui assenza non consentirebbe di “svolgere un compito specifico svolto nell'interesse pubblico esplicitamente previsto dalla legge” come la gestione del traffico;
3. l'ente pubblico “abbia esaurito tutti gli altri mezzi a sua disposizione per ottenere tali dati”.
In queste situazioni, il Data Act offre un abilitante giuridico per il settore pubblico che permette l'accesso ai dati su veicoli e conducenti.

Il processo specifico per fare richiesta di condivisione è descritto nell'*articolo 17* e risulta molto laborioso, mettendo in evidenza sia il timore verso la condivisione sproporzionata di dati che il rispetto degli “obiettivi legittimi del titolare dei dati, tenendo conto della tutela dei segreti commerciali e dei costi e degli sforzi necessari per mettere a disposizione i dati”. Per di più, la normativa favorisce la condivisione di dati non personali, presumibilmente per prevenire il fenomeno della profilazione.

Quando le autorità pubbliche ottengono i dati, devono rispettare diversi obblighi previsti dall'*articolo 19*. Per prima cosa, non è consentito usare i dati in maniera non coerente con la finalità per la quale sono stati raccolti. Inoltre, è molto importante che vengano prese le necessarie precauzioni per tutelare “la riservatezza e l'integrità dei dati richiesti e la sicurezza dei trasferimenti dei dati, in particolare dei dati personali” e “i diritti e le libertà degli interessati”. In seguito, i dati dovranno essere eliminati quando non più indispensabili per il motivo per il quale sono stati domandati, informando sia il titolare che coloro che li hanno ricevuti.

Seguendo il modello stabilito per la condivisione B2B, i dati non possono essere sfruttati a fini economici. Nel caso di emergenze pubbliche, i dati devono essere accessibili in modo gratuito e verrà riservato un riconoscimento pubblico al titolare nel caso lo richiedesse, mentre per altre motivazioni legali il compenso non eccede i costi necessari all'adempimento della richiesta.

Nel suo intento di favorire un sistema di condivisione maggiormente valido e interoperabile, l'*articolo 23* si propone di potenziare le condizioni per l'interoperabilità semantica dei dati tra diverse imprese, assicurando la libera circolazione dei consumatori nel mercato. In questo si favorisce la concorrenza ma allo stesso tempo si stabiliscono controlli di mercato. Tale norma è specificatamente orientata a garantire che l'interoperabilità tra imprese, compagnie assicurative e tra imprese e compagnie assicurative sia agevole e possa rendere più semplice l'accesso di prima parte ai dati EDR, oltre che quello di terze parti senza disagi o ostacoli ingiustificati. Conformemente alle prescrizioni dell'*articolo 23*, l'*articolo 28* si concentra sul consolidamento dei requisiti di interoperabilità sui dati EDR dentro le imprese come case automobilistiche e compagnie assicurative, secondo le richieste del cliente o la collaborazione interna tra imprese fondata sull'approvazione legittima dell'interessato. Questo influisce su una circolazione dei dati tra imprese senza vincoli e compatibile dal punto di vista tecnico.

3.4 Data Governance Act

Entrato in vigore nel Giugno 2022 e reso operativo nel Settembre del 2023, il Data Governance Act (DGA) è un regolamento il cui scopo fondamentale è quello di offrire un'alternativa alle modalità di gestione dei dati adottate dai colossi tecnologici, i quali continuano ad avere un notevole potere di mercato. L'intento è quello di favorire una ripartizione maggiormente bilanciata dei vantaggi derivanti dai dati, tanto in campo privato quanto in quello pubblico e lo si può intendere dai suoi obiettivi di

1. perfezionare le condizioni relative alla condivisione dei dati nel mercato locale, soprattutto tramite l'incremento della fiducia;
2. promuovere un contesto competitivo per la condivisione dei dati.

Per conseguire tale scopo, la legge intende stabilire un contesto normativo equilibrato per gli intermediari di dati neutrali e indipendenti da ogni altro tipo di servizio offerto, facilitando così la condivisione dei dati. La forma che possono assumere gli intermediari è quella di mercati di dati commerciali o organizzazioni di altruismo dei dati. In quest'ottica, l'aspirazione del DGA è paragonabile allo sviluppo infrastrutturale: l'UE presuppone in maniera implicita che, così come le reti di telecomunicazione agevolano lo scambio di informazioni, allora l'istituzione di un sistema normativo per gli intermediari darà vita a un mercato robusto per i servizi di intermediazione. In aggiunta, l'approccio ambizioso risulta anche nel vasto campo di applicazione in quanto riguarda tanto i dati personali quanto quelli non personali, in ogni settore, arrivando dunque a coprire per intero l'economia dei dati.

In particolare, il terzo capitolo del DGA è quello che definisce le norme per la creazione di *servizi di intermediazione dei dati*. Quest'ultimo si riferisce a “servizi finalizzati a instaurare, attraverso strumenti tecnici, giuridici o di altro tipo, rapporti commerciali ai fini della condivisione dei dati tra un numero indeterminato di interessati e di titolari dei dati, da un lato, e gli utenti dei dati, dall'altro”. All'interno del DGA, il termine *condivisione dei dati* è definito come “la fornitura di dati da un interessato o un titolare dei dati a un utente dei dati ai fini dell'utilizzo congiunto o individuale di tali dati, sulla base di accordi volontari o del diritto dell'Unione o nazionale, direttamente o tramite un intermediario, ad esempio nel quadro di licenze aperte o commerciali, dietro compenso o a titolo gratuito”.

Rientrano nella prima categoria quei “servizi di intermediazione tra i titolari dei dati e i potenziali utenti dei dati, compresa la messa a disposizione di mezzi tecnici o di altro tipo per consentire tali servizi; tali servizi possono includere scambi di dati bilaterali o multilaterali o la creazione di piattaforme o banche dati che consentono lo scambio o l'utilizzo congiunto dei dati, nonché l'istituzione di altra infrastruttura specifica per l'interconnessione di titolari dei dati con gli utenti dei dati”. Questa tipologia riflette il sistema dei data marketplace ed è coerente con l'allusione alla logica di mercato della condivisione, presente nella descrizione del concetto di servizi di intermediazione, all'interno della quale la condivisione funge da preludio ad una circolazione senza vincoli. In qualità di operatori di servizi di data sharing, dovrebbero abbattere i costi di transazione, integrando le fonti di dati e facilitando il collegamento tra utenti e fornitori.

Mentre la prima categoria concerne il legame tra titolari e utenti, la seconda riguarda il rapporto tra interessati e utenti. Nello specifico si tratta di “servizi di intermediazione tra interessati che intendono mettere a disposizione i propri dati personali o persone fisiche che intendono mettere a disposizione dati non personali e potenziali utenti dei dati, compresa la messa a disposizione di mezzi tecnici o di altro tipo per consentire tali servizi, permettendo in particolare l'esercizio dei diritti degli interessati di cui al regolamento (UE) 2016/679”. Quindi si tratta di fornitori che dovrebbero offrire i loro servizi al fine di potenziare l'autonomia decisionale degli interessati e, nello specifico, il potere di gestione dei dati, piuttosto che per lo scopo di elaborare i dati o accrescerne il valore. Questi fornitori supportano ogni individuo nell'attuazione dei loro diritti secondo quanto previsto dal GDPR: sono loro a dover gestire autorizzazione e revoca del consenso al trattamento dei dati, oltre all'attuazione dei diritti sanciti dal GDPR.

Alla terza ed ultima categoria appartengono le cooperative di dati. In base al *punto 31* del DGA, queste cooperative hanno l'obiettivo di potenziare la posizione dell'individuo (come nella categoria precedente), in modo tale che effettui delle scelte consapevoli prima di dare il consenso all'uso dei dati, condizionando termini e condizioni, definiti dalle organizzazioni di utenti di dati, che regolano l'uso degli stessi. Sempre le cooperative potrebbero inoltre fungere da strumento utile nei confronti di imprese individuali, micro, piccole e medie imprese, le quali sono tipicamente paragonabili al singolo individuo per quanto riguarda le competenze sulla condivisione dei dati.

Anche se queste cooperative sono inserite nella lista dei servizi di intermediazione, la norma specifica che la natura commerciale rappresenta la caratteristica distintiva di questi servizi e che “i servizi che ottengono dati dai titolari dei dati e li aggregano, arricchiscono o trasformano al fine di aggiungervi un valore sostanziale e concedono licenze per l'utilizzo dei dati risultanti agli utenti dei dati, senza instaurare un rapporto commerciale” non rientrano in tale contesto.

Le condizioni e gli obblighi fissati ai fornitori di servizi di intermediazione, sono significativamente più stringenti rispetto a quelli previsti per gli attori commerciali di altri settori. Prima di poter accedere al mercato, devono inviare una notifica all'autorità nazionale competente, con all'interno informazioni dettagliate, tra cui stato giuridico, struttura proprietaria e filiali di rilievo. In aggiunta, devono rispettare un gruppo di condizioni fondamentali stabilite dall'*articolo 12*. Per prima cosa, questi servizi di intermediazione devono essere del tutto indipendenti da ogni altra attività commerciale nella quale possano essere coinvolti. Questo aspetto si manifesta nei seguenti vincoli:

1. i servizi di intermediazione si devono erogare attraverso un'entità legale distinta;
2. il fornitore del servizio non può impiegare i dati scambiati per altri fini;
3. i metadati acquisiti mediante l'erogazione del servizio si possono usare esclusivamente per ottimizzare quest'ultimo;
4. le condizioni di vendita proposte ai beneficiari del servizio non devono essere influenzate dal fatto che i beneficiari usino altri servizi proposti dal fornitore del servizio o da un'altra entità collegata.

Pertanto, il DGA mira a favorire la nascita di intermediari di dati che agiscono in maniera differente rispetto alle principali piattaforme digitali. Gli operatori che offrono servizi di intermediazione sono obbligati a distinguere questi servizi dalle altre attività commerciali in cui sono coinvolti e non

possono ottenere vantaggi privati dai dati scambiati. Questo implica una netta discontinuità rispetto ai metodi delle attuali piattaforme digitali, le quali sono contraddistinte da potere monopolistico e decisioni autonome che incidono negativamente su rivali e clienti ed intralciano le iniziative normative. La concezione degli intermediari di dati proposta dal regolamento consiste in canali che permettono il collegamento tra acquirenti e venditori, senza avere il permesso di trarre alcun beneficio dai servizi di intermediazione, salvo la retribuzione economica per la prestazione dei servizi.

Per di più, il DGA richiede ben oltre che una basilare neutralità commerciale, infatti il *punto m) dell'articolo 12* stabilisce che l'intermediario “che offre servizi agli interessati agisce nell'interesse superiore di questi ultimi nel facilitare l'esercizio dei loro diritti, in particolare informandoli e, se opportuno, fornendo loro consulenza in maniera concisa, trasparente, intelligibile e facilmente accessibile sugli utilizzi previsti dei dati da parte degli utenti dei dati e sui termini e le condizioni standard cui sono subordinati tali utilizzi, prima che gli interessati diano il loro consenso”. Quindi, anche se si tratta di operatori commerciali che mettono in contatto compratori e venditori, sono obbligati a tutelare gli interessi della controparte più vulnerabile, ossia gli interessati.

Il quarto capitolo del regolamento definisce delle norme per le *organizzazioni di altruismo dei dati*. Il *punto 16 dell'articolo 2* presenta la seguente definizione del termine *altruismo dei dati*: “la condivisione volontaria di dati sulla base del consenso accordato dagli interessati al trattamento dei dati personali che li riguardano, o sulle autorizzazioni di altri titolari dei dati volte a consentire l'uso dei loro dati non personali, senza la richiesta o la ricezione di un compenso che vada oltre la compensazione dei costi sostenuti per mettere a disposizione i propri dati, per obiettivi di interesse generale”. Quindi si distingue per l'assenza di stimoli economici e il raggiungimento di scopi di interesse collettivo come il contrasto del cambiamento climatico, il potenziamento dei servizi pubblici, la salute pubblica, la ricerca scientifica e non solo.

Come per i fornitori di servizi di intermediazione, anche le organizzazioni di altruismo dei dati sono tenute ad osservare delle condizioni per effettuare la registrazione. Nello specifico, devono essere fondate nella forma di persona giuridica in conformità con il diritto nazionale per perseguire fini di carattere pubblico, devono agire senza finalità di lucro ed essere giuridicamente autonome da ogni organizzazione con obiettivo lucrativo. In aggiunta, devono effettuare le loro operazioni di altruismo mediante una struttura funzionalmente distinta da tutte le altre iniziative. Oltre a queste condizioni, sono obbligati a seguire specifici criteri di trasparenza durante l'esecuzione della loro prestazione. In dettaglio, devono mantenere registri dettagliati in merito a individui o persone giuridiche che hanno l'autorizzazione per trattare i dati, la durata e la finalità del trattamento, oltre che potenziali compensi versati da parte del beneficiario dei dati. Infine, dovrà consegnare questi registri all'ente nazionale preposto.

All'interno dell'*articolo 21*, vengono elencati dei requisiti da rispettare al fine di preservare i diritti e gli interessi di interessati e titolari dei dati. L'organizzazione che offre servizi di altruismo “informa in maniera chiara e facilmente comprensibile gli interessati o i titolari dei dati, prima di qualsiasi trattamento dei loro dati” relativamente “agli obiettivi di interesse generale e, se opportuno, alla finalità determinata, esplicita e legittima per cui i dati devono essere trattati”.

Inoltre, risulta molto importante che non usi i dati per altre finalità differenti da quelle di interesse generale per le quali gli interessati o i titolari dei dati acconsentono al trattamento e che non adotti “pratiche commerciali ingannevoli per sollecitare la fornitura di dati”. In aggiunta, devono coinvolgere attivamente tanto gli interessati quanto i titolari, riguardo ai loro dati, per mezzo di “strumenti per ottenere il consenso degli interessati o le autorizzazioni al trattamento dei dati messi a disposizione dai titolari dei dati” e di “strumenti per l'agevole revoca di tale consenso o autorizzazione”.

Capitolo 4-Cybersecurity e Privacy

L'ingresso nel settore automotive da parte di veicoli dotati di accesso ad Internet, scambio di dati e aiuti alla guida segna una trasformazione significativa rispetto alla tradizionale rappresentazione di un'automobile. In particolare, le vetture moderne sono in grado di acquisire e condividere dati con altri dispositivi grazie a sistemi innovativi di cui sono equipaggiati. Oltre ad una migliore esperienza al volante, questa evoluzione costituisce un passo cruciale nell'avanzamento tecnologico delle vetture. Nonostante questi aspetti positivi, l'incremento di connettività a bordo pone importanti questioni legate alla sicurezza informatica, tra cui tentativi di accesso non consentito, compromissione dei dati e la possibilità di controllo da remoto non autorizzato. Questi sono alcuni esempi di criticità che mettono in evidenza l'urgente bisogno di implementare sistemi di protezione avanzati per tutelare i veicoli connessi da eventuali attacchi informatici. Dal momento che un ruolo chiave è giocato dalle tecnologie di comunicazione, la priorità assoluta è quella di garantire la sicurezza delle loro connessioni, in quanto rappresentano un bersaglio per i malintenzionati che vogliono ottenere dati o provocare danni. Confrontando la sicurezza informatica dei veicoli connessi con quella tradizionale, quest'ultima risulta differente sotto certi punti di vista. In particolare, gli utenti finali devono sostenere un carico di responsabilità superiore. Nei veicoli connessi, invece, la cybersecurity deve essere presente a partire dalla fase di progettazione data la complessità nell'applicare eventuali aggiornamenti di sicurezza. Quando si parla di protezione delle vetture connesse, si comprende sia la tutela della riservatezza dei dati trasmessi, al fine di evitare accessi non consentiti, che l'individuazione di informazioni dannose o errate che andrebbero a compromettere il funzionamento del mezzo di trasporto.

Esistono molteplici e diversificate minacce che mettono a rischio la sicurezza delle automobili connesse, però la quasi totalità può essere suddivisa in due categorie principali. La prima è quella degli *attacchi alla rete di bordo*, ovvero quelli nei quali l'aggressore si serve della connessione tra le varie componenti interne all'auto. Nello specifico, si manifestano attraverso la comunicazione non adeguatamente protetta tra i vari sistemi del veicolo. Gli *attacchi alla rete vehicle to everything (V2X)* rappresentano la seconda tipologia e tipicamente hanno come punto di ingresso la connessione tra veicolo e reti esterne. Per quanto riguarda il bersaglio, possono colpire la vettura stessa oppure il sistema esterno a cui è connessa. Di conseguenza, questi attacchi risultano più spinosi da contrastare e potrebbero avere conseguenze ben peggiori.

In linea generale, la conseguenza di un attacco alla rete di bordo è l'invio di dati distorti ai sensori, i quali ricevendo degli input inesatti, generano degli output inaffidabili. Ad esempio, il conducente potrebbe visualizzare sul cruscotto dei valori sbagliati riguardo alla temperatura del motore oppure alla velocità del veicolo. In ogni vettura è presente il debimetro, ovvero un sensore che misura la quantità d'aria fornita al motore e le cui informazioni sono utilizzate dal modulo di controllo della potenza al fine di stabilire la quantità di carburante da iniettare nel motore tenendo in considerazione elementi come i giri del motore e la posizione dell'acceleratore. Chiaramente si tratta di un sensore critico, il cui malfunzionamento potrebbe compromettere la corretta operatività del motore che riceverebbe carburante in eccesso oppure insufficiente.

Un ulteriore esempio di attacco alla rete di bordo riguarda la centralina elettronica, Electronic Control Unit (ECU) che svolge un ruolo cruciale in quanto monitora e gestisce diversi componenti e sistemi

di un mezzo, tra cui motore, iniezione del carburante, emissioni, sistemi avanzati di assistenza alla guida o ADAS, servosterzo, cambio e non solo. L'interazione tra ECU e i suddetti sistemi avviene tramite dei sensori che inviano i dati acquisiti alla ECU, la quale li elabora per definire delle istruzioni che gli attuatori del veicolo convertono in azioni fisiche. All'interno della ECU si trovano sensori di input, memorie, un microprocessore e circuiti di output. Di conseguenza risulta necessario che rimanga al passo con le ultime tecnologie e per farlo bisogna effettuare l'operazione chiamata flashing del software della ECU, ovvero la riprogrammazione che comprende progettazione, consegna ed installazione del software. Il problema risiede nel fatto che esistono degli attacchi diretti al flashing del software ECU tra cui la modifica del codice che può alterare le informazioni e compromettere le performance della parte hardware e il reverse engineering che può comportare la diffusione di informazioni preziose.

Tra gli specialisti di tecnologia, l'attacco alla rete V2X maggiormente familiare è l'attacco DoS acronimo di Denial of Service. Quest'ultimo è molto diffuso per la facilità con cui lo si mette in atto. La diretta conseguenza è un notevole peggioramento della connessione internet della rete interessata. Ragionando in ottica di veicoli autonomi, un ritardo nello scambio di comunicazioni tra i sensori della vettura e quelli del software che interpreta gli input che riceve, potrebbe causare gravi incidenti con possibili vittime.

Appartiene alla stessa tipologia anche l'attacco di falsificazione dei dati, che consiste nell'invio di informazioni errate all'automobile. Chiaramente riguarda soprattutto le assicurazioni e le forze dell'ordine che utilizzano le informazioni acquisite dal veicolo al fine di evitare potenziali pericoli futuri o per stabilire la dinamica di un sinistro.

Con lo scopo di gestire i rischi di natura informatica legati ai veicoli connessi, esistono diverse strategie di mitigazione che si possono suddividere in *riservatezza*, *integrità* e *disponibilità*, i quali rappresentano i tre pilastri della cybersecurity.

Una prima misura per tutelare la *riservatezza* dei dati è l'*autenticazione* che permette di verificare se un utente o una macchina abbiano l'autorizzazione per effettuare l'accesso ad un sistema. Per evitare che venga elusa, l'autenticazione dovrebbe avvalersi di metodi crittografici adeguati a gestire i dati di autenticazione. Infine, non dovrebbe usare semplicemente nome utente e password, ma dovrebbe attivare l'autenticazione a più fattori.

La *crittografia* è la seconda e consente di evitare che utenti o macchine interpretino dati che hanno acquisito senza autorizzazione. Le tecniche di crittografia possono essere leggere nel caso di sistemi con ridotte capacità oppure intensive necessitando così di una quantità superiore di risorse computazionali. Tenendo in considerazione il fatto che all'interno dei veicoli connessi, sono presenti sistemi che trasmettono ed elaborano i dati in maniera rapida, le tecniche crittografiche leggere sono spesso le più consone.

Tanto l'autenticazione quanto la crittografia possono supportare la prevenzione dell'alterazione dell'integrità dei dati, ma, nonostante ciò, esistono altre misure più indicate per l'*integrità* come i controlli di coerenza. I *checksum crittografici* sono usati per controllare se un messaggio o un dato abbia subito delle alterazioni. Un aggressore può eludere questa misura nel caso in cui identifica il

tipo di checksum, perché può generare messaggi che superino questo controllo. Eppure, rimane una complessità ulteriore che potrebbe dissuadere eventuali malintenzionati.

Inoltre, si possono effettuare dei *controlli di portata e velocità* che sono in grado di garantire che i messaggi o i dati siano corretti attraverso il confronto tra portata e velocità della sorgente dalla quale arrivano dati o messaggi e portata e velocità attesi della sorgente.

Dato che gli automobilisti dipendono in maniera crescente dalle funzionalità di cui sono dotati i veicoli connessi, la disponibilità ricopre un ruolo cruciale. Ad esempio, se i vari sistemi avanzati di assistenza alla guida non fossero disponibili, si andrebbe a compromettere di molto la sicurezza.

Una soluzione al tema della cybersecurity arriva proprio dall'Italia, dove alla fine del 2022 è nato il *Global Automotive Security Test Center* di NTT DATA appartenente al gruppo Nippon Telegraph and Telephone (NTT). Nello specifico si tratta di un centro che consente ai clienti che si trovano in uno dei paesi in cui opera il gruppo, di effettuare dei test di sicurezza sulle loro auto con l'obiettivo di tutelarne i sistemi da possibili cyberattacchi. Marco Garelli, colui che ricopre il ruolo di Head of Automotive di NTT Data Italia, ha dichiarato che "Vogliamo applicare le nostre competenze maturate nel mondo della cybersecurity al settore delle auto connesse. Grazie al Centro di test diventiamo un punto di riferimento a livello internazionale per proteggere i veicoli da attacchi cyber e garantire la sicurezza dei guidatori". Nel dettaglio, il centro impiega il 'System Level Fuzz Testing', ovvero una metodologia che permette di individuare bug e debolezze all'interno del software delle centraline delle auto. Oltre a ciò, c'è la possibilità di richiedere la 'Anomaly Detection' che è in grado di individuare possibili anomalie nelle comunicazioni tra le centraline del mezzo. Quest'ultima è una soluzione innovativa in quanto adopera l'intelligenza artificiale per avvisare di un possibile attacco in atto e mandare un segnale ad un centro di controllo capace di intervenire tempestivamente.

Di seguito alcuni eventi che testimoniano la rilevanza del tema della cybersecurity e della privacy in ambito automotive.

Tra quelli che si sono susseguiti negli anni, il primo ad aver messo in evidenza il tema della sicurezza informatica a bordo delle vetture è il caso *dell'esperimento condotto da Chris Valasek e Charlie Miller* nel 2015. Questi due specialisti della cybersecurity avevano già condotto un esperimento simile nel 2013 anche se in quel caso l'operazione di hacking era avvenuta a bordo dell'auto e con un laptop direttamente collegato al terminale diagnostico della vettura. Invece, nel secondo esperimento, l'accesso non autorizzato è stato effettuato sempre con un computer portatile ma questa volta da remoto a diversi chilometri di distanza, adoperando dei punti deboli del sistema Uconnect, di cui erano dotate le vetture del gruppo Fiat Chrysler (FCA). Questo sistema era utilizzato per gestire qualche funzionalità del veicolo da remoto sfruttando una rete cellulare per mantenere il mezzo costantemente connesso a Internet. Di conseguenza, i proprietari potevano interagire in qualsiasi momento con il loro veicolo e inviare comandi quali ad esempio l'accensione o lo spegnimento del motore, rendere operativo l'antifurto, visualizzare le informazioni diagnostiche e localizzare la posizione tramite il GPS integrato. Una volta che i due hacker sono entrati nel sistema Uconnect, hanno acquisito il numero identificativo, la posizione e l'indirizzo IP. In pochissimo tempo, sono riusciti a compromettere il funzionamento di vari comandi dell'automobile guidata dal giornalista Andy Greenberg. Queste sono alcune dichiarazioni del giornalista dopo che l'esperimento era

terminato: “Immediatamente il mio acceleratore ha smesso di funzionare. Ho freneticamente premuto il pedale e ho guardato la salita RPM (giri del motore), la Jeep ha perso metà della sua velocità e ha poi rallentato a passo d'uomo. Ciò è avvenuto proprio in prossimità di un lungo cavalcavia, non avevo via di fuga. L'esperimento non era più così divertente. Mentre i due hacker prendevano il controllo dell'aria condizionata, della radio e dei tergicristalli, mi congratulavo con me stesso per il mio coraggio”. Chiaramente, essendo un test controllato non ci sono state conseguenze negative. Inoltre, FCA era a conoscenza di questa prova e nello stesso anno ha fornito un aggiornamento software da installare nel veicolo ad opera degli stessi clienti tramite una chiavetta usb.

Un altro caso rappresentativo è quello della casa automobilistica *Toyota* che ha interessato approssimativamente 2,15 milioni di veicoli e nel quale a seguito di un involontario errore umano, i dati riguardanti il servizio T-Connect dello stesso produttore, sono stati resi accessibili a tutti anziché condivisi in maniera privata (il cloud è stato configurato come pubblico invece che privato). Secondo quanto riferito dal produttore di automobili giapponese, tali dati sono rimasti accessibili al pubblico all'incirca per un decennio, sin dal Novembre 2013. Nello specifico, sono coinvolti i proprietari che hanno fatto uso delle piattaforme cloud di punta della casa automobilistica e che hanno aderito ai servizi nel periodo compreso tra Gennaio 2012 e Aprile 2023, inclusi i clienti Lexus che hanno usufruito del servizio simile G-Link. La Toyota ha dichiarato di essersi resa conto dell'avvenuta violazione di dati relativi a clienti giapponesi soltanto ad Aprile 2023. Il sistema cloud trasmette dati quali la localizzazione del veicolo e i codici identificativi dei dispositivi della vettura. Una moltitudine di servizi è compresa nella piattaforma T-Connect come il supporto alla guida tramite intelligenza artificiale, il collegamento automatico ai centri di assistenza per il veicolo e il supporto per le emergenze. Per rimediare ed evitare che riaccada un evento analogo, Toyota ha dichiarato che adotterà misure preventive. In particolare, implementerà un sistema di controllo sulle impostazioni del cloud e punterà a migliorare la formazione del personale riguardo alla gestione dei flussi di dati, introducendo un sistema che monitori in maniera costante le impostazioni chiave del cloud. Infine, ha affermato di aver intrapreso un'indagine approfondita in ognuno dei propri ambienti cloud e che, una volta che la criticità è stata rilevata, sono stati presi provvedimenti tempestivi al fine di impedire accessi esterni non autorizzati.

Ad Aprile 2023, la casa automobilistica sudcoreana *Hyundai* ha dichiarato di essere stata vittima di un attacco informatico tramite il quale alcuni criminali sono riusciti a entrare in possesso di dati relativi a clienti di Italia e Francia. La portata dell'evento non è stata assolutamente limitata, in quanto le vendite di vetture Hyundai in Europa ammontano all'incirca a 500 mila ogni anno. Inoltre, i dati interessati non solo riguardavano clienti ordinari ma anche quelli occasionali come coloro che avevano semplicemente richiesto un test drive. Sulla base delle e-mail ricevute dai clienti e che sono state successivamente pubblicate sui social network, tra le informazioni compromesse sono incluse quelle relative alla vettura come il numero di telaio, indirizzi e-mail, numeri di cellulare e indirizzo di residenza. Inoltre, dalla comunicazione ufficiale del produttore di automobili si evince che il furto ha avuto come oggetto 'esclusivamente' dati anagrafici e non quelli di natura finanziaria.

Sempre la Hyundai, in particolare la divisione europea (Hyundai Motor Europe) è stata colpita da un attacco informatico a Gennaio del 2024. La casa automobilistica sudcoreana non ha ancora pubblicato dettagli sull'accaduto, ma stando a quanto riportato dal rapporto di BleepingComputer (un sito di

notizie relative alla cybersecurity) l'autore del gesto è il gruppo di hacker Black Basta che esegue attacchi informatici con lo scopo di estorcere denaro tramite riscatto. Nel suddetto caso, è riuscita ad acquisire senza autorizzazione 3 terabyte di dati. Anche se non risulta ancora quali siano i dati interessati, la BleepingComputer dichiara di aver visionato immagini fornite dall'aggressore che mostrano cartelle, i cui nomi suggeriscono che siano legate a diversi dipartimenti della Hyundai Motor Europe, compresi risorse umane, vendite, management, contabilità, legale e IT. Ciò che sorprende maggiormente, è il fatto che la BleepingComputer era al corrente dell'attacco già a Gennaio e nel momento in cui ha provato a chiedere chiarimenti alla Hyundai, quest'ultima ha affermato che si trattava di semplici problemi informatici. Però, quando successivamente il suddetto sito web ha iniziato a condividere informazioni a loro disposizione relative all'evento, allora il produttore di automobili ha confessato alla stessa BleepingComputer che "Hyundai Motor Europe sta indagando su un caso in cui una terza parte non autorizzata ha avuto accesso a una parte limitata della rete di Hyundai Motor Europe" (<https://www.bleepingcomputer.com/news/security/hyundai-motor-europe-hit-by-black-basta-ransomware-attack/>).

Riguardo ai rischi per la privacy, un chiaro segnale di allarme arriva dallo *studio condotto da Mozilla Foundation*, un'organizzazione globale senza scopo di lucro che dal 2017 controlla il trattamento dei dati in numerose tipologie di prodotti. Essa *ha esaminato la cura della Privacy da parte di 25 case automobilistiche riguardo ai dati raccolti su veicoli e persone a bordo*. Da diverso tempo le aziende produttrici di automobili affermano che le loro auto sono dei veri e propri 'computer su ruote' al fine di pubblicizzare le caratteristiche tecnologiche avanzate dei veicoli che mettono in commercio. Uno dei primi ad utilizzare questo termine fu proprio Elon Musk, che durante la presentazione dell'aggiornamento software per la Model S, nel 2015 affermò che lo sviluppo di questo modello è stato realizzato al fine di renderlo un "computer molto sofisticato su ruote". Inoltre, uno degli analisti del settore automotive operante presso Standard&Poor's Capital IQ, affermò sempre nello stesso anno, che si stava verificando una sorta di "convergenza tra auto e telefono cellulare". Si può dire che in poco tempo, le case automobilistiche hanno fatto il loro ingresso nel mercato dei dati, rendendo le loro vetture dei dispositivi capaci di raccogliere enormi quantità di dati. Infatti, con le varie funzionalità di cui sono dotate, possiedono un'incomparabile abilità nell'osservare, ascoltare e memorizzare informazioni riguardo alle attività del conducente, i luoghi che frequenta con l'auto e non solo.

Di seguito, le conclusioni della sopracitata ricerca.

1. Per prima cosa, il 100% dei 25 produttori di auto ha ricevuto l'avviso *Privacy Not Included, testimoniando il fatto che secondo la Mozilla Foundation le autovetture hanno rappresentato la tipologia di prodotto più problematico per la privacy rispetto a qualsiasi prodotto esaminato in precedenza.
2. Tutte le case automobilistiche analizzate acquisiscono un volume di dati di gran lunga superiore rispetto a quanto indispensabile e lo sfruttano per finalità differenti da quelle necessarie come rendere operativo il mezzo e gestire il rapporto con il conducente. Ad oggi, possono usufruire di varie possibilità per l'acquisizione di dati in confronto ad altri prodotti e app, persino più delle soluzioni smart per la casa o degli smartphone. Come già illustrato nei capitoli precedenti, sono in grado di ottenere informazioni personali attraverso l'interazione

con il veicolo, i servizi connessi, l'applicazione del marchio automobilistico che agisce come 'punto di accesso' per i dati sul telefono e da fonti esterne come Google Maps. Il problema principale riguarda le informazioni estremamente personali a cui possono accedere, incluse quelle mediche, genetiche e quelle sulla sfera intima, passando ad altre meno personali come velocità, localizzazione geografica e brani musicali. Tutti questi dati vengono tipicamente sfruttati per arrivare ad ulteriori deduzioni sul conducente (questo processo si chiama *inferenza*) come interessi, abilità tecniche e livello di intelligenza ad esempio.

3. Oltre alle grandi quantità di dati personali che possiedono queste aziende, risulta molto preoccupante che ben l'84% di esse abbia dichiarato di avere la possibilità di condividerli liberamente con terze parti, tra cui broker di dati, imprese che offrono servizi ed altre aziende. Come se non bastasse, il 76% sostiene di poterli addirittura vendere. Infine, poco più della metà (56%) rivela che in seguito ad una sorta di 'richiesta', è in grado di metterli a disposizione di istituzioni governative e forze dell'ordine.
4. La quasi totalità (92%) non permette ai conducenti un sufficiente potere decisionale sui dati che li riguardano. Le case automobilistiche che si salvano sono Renault e Dacia, le quali garantiscono in maniera imprescindibile il diritto di cancellazione. La motivazione risiede nel fatto che entrambe operano esclusivamente nel mercato europeo, dove vige il Regolamento generale sulla protezione dei dati (GDPR).
5. Non è stato possibile stabilire con esattezza se qualcuna delle aziende esaminate rispetti i requisiti minimi di sicurezza della Mozilla Foundation. Inoltre, i ricercatori di questo studio hanno tentato di entrare in contatto con queste aziende, mandando delle e-mail nelle quali chiedevano spiegazioni, ma buona parte non li ha presi in considerazione ad eccezione di Ford, Mercedes e Honda anche se non sono state in grado di fornire risposte esaustive a domande concernenti la sicurezza di base. Infine, al 68% delle imprese esaminate è stato assegnato l'avviso 'bad track record' a causa di violazioni che hanno messo a rischio la privacy dei loro conducenti, attacchi cibernetici e divulgazioni non autorizzate. Lo confermano i casi di violazioni precedentemente illustrati.
6. A dimostrazione di quanto sia complesso l'argomento, i ricercatori affermano di aver dedicato oltre 600 ore di tempo per esaminare le politiche sulla privacy dei produttori di auto, quando di norma ne impiegano 200. Malgrado il notevole sforzo, in nessun caso le politiche sulla privacy hanno fornito una visione chiara e completa delle finalità e modalità con cui sono condivisi i dati acquisiti. Considerato ciò, i 3 ricercatori si sono chiesti come un qualsiasi individuo possa comprendere la questione precedentemente citata se neppure loro sono stati in grado di comprenderla in qualità di specialisti della privacy.
7. Un altro aspetto curioso riguarda il consenso, in particolare per la Subaru, che all'interno della sua policy sulla privacy, sostiene che i passeggeri di un'autovettura dotata di servizi connessi danno il consenso per usare e vendere le proprie informazioni personali banalmente per il fatto di trovarsi a bordo del veicolo.

Leggermente diverso è il caso di Tesla, la quale concede all'utente la possibilità di annullare la raccolta dati, anche se ci tiene a precisare che questa scelta potrebbe causare una funzionalità ridotta, seri danni o addirittura rendere non operativa la vettura.

Un caso simile alla Subaru è quello della Nissan, la quale affida al guidatore stesso il compito di istruire e informare le persone a bordo del veicolo riguardo alle politiche sulla privacy. Di

conseguenza, il guidatore sarebbe tenuto a leggere un testo lungo poco meno di 10000 parole a ogni persona nell'abitacolo.

Dalle suddette conclusioni, la Mozilla Foundation ha realizzato la tabella sottostante, la quale mostra come le case automobilistiche (classificate dalla “migliore” alla peggiore) si comportano rispetto ai criteri di privacy, sicurezza, tutela dei dati, raccolta esagerata di dati non strettamente necessari e come meglio definiti dalla Mozilla Foundation per i criteri di seguito elencati:

- *Data use* si riferisce all'utilizzo dei dati acquisiti sugli utenti da parte delle case automobilistiche. In questa colonna compare la X nel caso in cui le suddette aziende raccolgano dati che non sono strettamente indispensabili al funzionamento del prodotto, oppure vendono o condividono con terzi, dati relativi agli utenti per scopi diversi dal funzionamento del prodotto. Tutte le 25 aziende sono state contrassegnate per il 'Data use' poiché raccolgono dati che vanno oltre lo stretto indispensabile.
- *Data control* riguarda il controllo che gli utenti possono esercitare sui loro dati. In particolare, se l'azienda mette a disposizione degli utenti un metodo semplice e trasparente per richiedere l'accesso o l'eliminazione dei propri dati oppure se illustra chiaramente il periodo di tempo di conservazione delle informazioni personali. Solamente Renault e Dacia non sono contrassegnate dalla X semplicemente perché sono case automobilistiche europee, le quali devono sottostare al Regolamento generale sulla protezione dei dati (GDPR), ma soprattutto non vendono auto in Nord America dove invece le norme sulla privacy sono decisamente più permissive. Infatti, grazie al GDPR, ogni utente possiede il diritto di accesso ed eliminazione dei propri dati, mentre negli Stati Uniti questi diritti non sono presenti.
- *Track record* è relativo alla presenza (X) o meno di eventi avvenuti negli ultimi 3 anni che testimoniano una scarca capacità di tutela dei dati da parte dell'azienda automobilistica come, ad esempio, violazioni del sistema di sicurezza e attacchi informatici.
- *Security* per stabilire se il prodotto considerato rispetta gli standard minimi di sicurezza definiti da Mozilla. Questi sono: crittografia, aggiornamenti di sicurezza, password robuste, gestione delle vulnerabilità, privacy policy. Riguardo alla crittografia, nessuna casa automobilistica ha dimostrato chiaramente di crittografare ogni dato personale che si trova a bordo della vettura. Se è presente la X, vuol dire che i suddetti standard non vengono rispettati.
- *Intelligenza artificiale* per valutare l'affidabilità, le attività che svolge, la trasparenza sul suo funzionamento da parte dell'impresa e se l'utente può controllare le sue funzionalità. L'unica casa automobilistica a ricevere una X è stata Tesla, a causa del pilota automatico AI-powered che è stato probabilmente coinvolto in 17 decessi e 736 incidenti negli Stati Uniti ed è ad oggi sottoposto a varie indagini governative.
- *Review* rappresenta una valutazione complessiva e viene assegnato quel triangolo con il punto esclamativo che rappresenta l'etichetta di avviso **Privacy Not Included* della Mozilla Foundation nel caso in cui il prodotto valutato viene attenzionato su 2 o più criteri di privacy e sicurezza.

Car brand	Data use	Data control	Track record	Security	AI	Review
	X			X		
	X			X		
	X	X		X		
	X	X		X		
	X	X		X		
	X	X		X		
	X	X		X		
	X	X		X		
	X	X	X	X		
	X	X	X	X		
	X	X	X	X		
	X	X	X	X		
	X	X	X	X		

	X	X	X	X		
 Mercedes-Benz	X	X	X	X		
 HONDA	X	X	X	X		
 ACURA	X	X	X	X		
	X	X	X	X		
 CHEVROLET	X	X	X	X		
 BUICK	X	X	X	X		
	X	X	X	X		
 CADILLAC	X	X	X	X		
 HYUNDAI	X	X	X	X		
 NISSAN	X	X	X	X		
 TESLA	X	X	X	X	X	

Nel 2023, *Ford* ha stupito il settore automotive con un singolare brevetto depositato negli Stati Uniti e che presenta una sorta di tecnologia di auto-recupero che opera tramite la connettività della vettura con la casa automobilistica, un ente creditizio, un'agenzia di recupero e un'autorità governativa.

All'interno del documento vengono elencati diversi disagi che potrebbero subire gli automobilisti non in regola con i pagamenti delle rate sull'auto. In particolare, nei primi giorni di ritardo il mezzo inizia semplicemente con il ricordare le scadenze dei pagamenti per poi passare a dei veri e propri interventi di disturbo. Tra questi si parla di compromettere il funzionamento di alcuni componenti come finestrini, sistema di infotainment, cruise control e la regolazione dei sedili. Dopo di che, il sistema andrebbe a colpire in maniera crescente elementi come, ad esempio, il sistema di climatizzazione e in seguito addirittura componenti quali blocco e sblocco automatico delle portiere. Inoltre, si aggiunge anche un suono continuo e fastidioso che si attiva ogni qualvolta il proprietario entra nell'abitacolo. Infine, nel caso in cui si tratti di un veicolo a guida autonoma o semi-autonoma, questo sistema di auto-recupero sarebbe in grado di muovere la vettura fino a un luogo che consenta al carro attrezzi di agganciarla in maniera agile oppure trasferirla dalla residenza del proprietario al deposito dell'agenzia di recupero. Nel caso estremo in cui l'ente creditizio ritenga antieconomico procedere con il recupero, la vettura verrebbe portata direttamente ad un centro di demolizione.

Tutte queste criticità stanno spingendo l'emergere di soluzioni che tutelino la privacy. Una di queste è stata realizzata da *Privacy4Cars*, un'azienda tecnologica focalizzata sull'identificare e risolvere problemi di privacy nel settore automotive. In particolare, ha sviluppato un innovativo strumento chiamato *Vehicle Privacy Report*, che mette a disposizione degli automobilisti una panoramica sulla tipologia e quantità di informazioni che le auto acquisiscono, semplicemente inserendo il numero di telaio nel sito web vehicleprivacyreport.com. Alla fine del 2023, Andrea Amico, il fondatore di *Privacy4Cars* ha annunciato l'espansione dello strumento al mercato europeo, sostenendo che nonostante i cittadini europei godano delle più rigide normative sulla privacy a livello mondiale, rimarrebbero sorpresi nel constatare la quantità di informazioni personali acquisite e condivise dalle case automobilistiche e quanto possa essere esteso il divario tra i requisiti imposti dalla legge e le pratiche commerciali. Come se non bastasse ha dichiarato che i risultati di una *loro ricerca* hanno mostrato che ben quattro auto su cinque in Europa, sono rimesse in vendita con all'interno dati sensibili e non crittografati dei consumatori, anche se i responsabili del trattamento (concessionari, leasing di flotte, compagnie assicurative) non godono di una base legale per trattarli e siano pertanto obbligati, secondo il GDPR a cancellarli. Infine, sempre il fondatore ha precisato che l'espansione del *Vehicle Privacy Report* ha come finalità quella di incrementare la trasparenza per i consumatori e supportarli nella difesa dei loro diritti in maniera gratuita. Non solo, in contemporanea tentano di fornire alle imprese produttrici di auto, l'occasione per dare prova di come integrano la privacy all'interno della proposta di valore e prestano più cura nei confronti dei clienti. A dimostrazione del grande lavoro svolto da *Privacy4Cars*, nel 2023 ha ottenuto il riconoscimento di 'European Start Up of the Year', confermandosi come punto di riferimento nel campo della privacy-tech all'interno dell'industria automobilistica internazionale.

Nelle righe successive maggiori dettagli della *ricerca sopracitata* dal fondatore di *Privacy4Cars* Andrea Amico. Per prima cosa, sono stati analizzati centinaia di veicoli in vendita al dettaglio e all'ingrosso tra il 2021 e 2024 in Germania, Italia e Regno Unito. Come già detto in precedenza, il risultato di questa analisi ha portato a concludere che quattro vetture su cinque sono rivendute con all'interno dati personali di precedenti proprietari.

Inoltre, nel periodo compreso tra Dicembre 2023 e Maggio 2024, alcuni acquirenti (uno per ogni concessionario) in incognito per conto di Privacy4Cars, si sono recati presso 46 concessionari del Regno Unito, fingendo di voler acquistare un veicolo usato. I finti clienti hanno chiesto ad ognuno dei concessionari se cancellassero i dati personali prima della vendita e 35 su 46 hanno risposto di sì, mentre 3 hanno dichiarato che li eliminano solo su richiesta ed i restanti 8 non hanno risposto in maniera chiara. I risultati sono differenti dalle affermazioni dei rivenditori poiché la meta degli acquirenti ha trovato informazioni sullo smartphone come chiamate e messaggi; invece, un terzo ha scoperto indirizzi di varie località. Presso quei rivenditori che dichiarano di rispettare il GDPR, sono stati effettuati un totale di 70 test drives e in 40 sono stati rinvenuti dati personali relativi ai passati proprietari.

A conferma del limitato grado di consapevolezza degli utenti sulla raccolta e il trattamento dei dati da parte delle case automobilistiche, è presente una ricerca richiesta dall'Ufficio europeo della Federazione Internazionale dell'Automobile (FIA). In questo lavoro del 2023 è stato analizzato un campione composto da 11.000 automobilisti di 11 Nazioni (Danimarca, Belgio, Spagna, Germania, Polonia, Finlandia, Austria, Repubblica Ceca, Francia, Italia e Paesi Bassi). L'obiettivo era quello di comprendere l'atteggiamento della popolazione europea nei confronti dei progressi tecnologici. Le conclusioni segnalano uno scenario per nulla rassicurante.

In primis, il 59% dei conducenti non è a conoscenza del fatto che guida un veicolo connesso e il 61% non ha memoria di aver concesso il consenso per l'acquisizione e il trattamento dei dati inerenti alla loro vettura.

Mentre il 47% è al corrente che i dati acquisiti dalle case automobilistiche siano raccolti e condivisi, il 59% esprime timori verso la mancanza di spiegazioni adeguate sull'impiego che se ne fa.

Lo studio, incentrato principalmente su fattori come libertà di scelta per il consumatore, rapidità nel fornire servizi e prezzi, ha rilevato che il 65% desidera poter sostituire il fornitore telematico della sua auto e il 61% di poterlo sostituire in qualsiasi momento della vita utile del proprio veicolo.

Per il 59%, colui che avrebbe il compito di mettere a disposizione una quantità superiore di servizi aggiuntivi connessi dovrebbe essere il produttore di automobili e non terze parti.

Il 62% è disponibile a cambiare il centro di assistenza della casa madre con uno privato, se quest'ultimo applica prezzi più convenienti. Mentre il 56% effettuerebbe questo cambio in presenza di tempi di intervento minori. Tra le altre motivazioni sono presenti l'accesso ai servizi da remoto (46%), pure tramite computer di bordo (42%) oppure attraverso app (41%).

Pressappoco un automobilista su tre (29%) sarebbe propenso a scaricare applicazioni non gratuite per la vettura, al contrario del 50% che si ritiene favorevole ad applicazioni gratuite accettando la ricezione di pubblicità mirate.

Per concludere, lo studio della FIA esamina le aspettative degli automobilisti riguardo alle normative europee sugli argomenti precedentemente citati.

Il 46% reputa che produrranno effetti positivi per la sicurezza sulle strade, il 43% si aspetta una più ampia varietà di servizi offerti e il 42% si augura che si innovino in maniera più rapida. Inoltre, il 35% spera che i prezzi dei servizi per i consumatori possano diminuire.

Data la continua diffusione delle auto connesse, la FIA afferma che sarà compito del Legislatore europeo promuovere questo progresso tecnologico, mantenendo sempre in considerazione le numerose e sensibili tematiche tutt'ora da approfondire per ciò che concerne raccolta ed utilizzo dei dati.

Da un punto di vista normativo, oltre al Regolamento generale sulla protezione dei dati (GDPR), risultano rilevanti le *Linee guida 01/2020*, essendo molto più specifiche visto che riguardano il trattamento dei dati personali nell'ambito dei veicoli connessi e delle applicazioni per la mobilità.

In riferimento ai dati personali, le linee guida si concentrano su quelli trattati nell'abitacolo del mezzo, condivisi tra vettura e dispositivi collegati ad essa come lo smartphone, acquisiti in loco nell'automobile e trasferiti ad organizzazioni esterne quali ad esempio enti assicurativi, case automobilistiche e centri di assistenza.

Nel campo di applicazione delle linee guida sono incluse le applicazioni mobili autonome rispetto al veicolo, chiamate 'stand-alone', come ad esempio quelle basate unicamente sull'uso dello smartphone. Tipicamente il loro scopo è quello di supportare i guidatori attraverso diverse funzionalità tra cui:

- Ottimizzazione degli spostamenti
- Gestione della vettura
- Svago
- Supporto alla guida
- Sicurezza stradale
- Comfort

Un aspetto che viene messo in risalto è quello relativo al consenso dell'utente che deve essere manifestato in maniera evidente.

Il documento si concentra su tre tipologie di dati personali:

- *Biometrici* - Sono impiegati per riconoscere senza ambiguità una persona e possono essere trattati al fine di permettere l'accesso a un mezzo, la verifica dell'identità del conducente o del proprietario e l'accesso alle preferenze del guidatore. Tutto ciò è consentito solo se è inclusa un'opzione non biometrica come una chiave e la custodia e la comparazione avvengono in forma cifrata esclusivamente a livello locale, escludendo trattamenti esterni.
- *Riguardanti l'ubicazione* – Questi possono essere acquisiti esclusivamente nel caso in cui sia strettamente indispensabile agli scopi del trattamento, in quanto forniscono informazioni relative allo stile di vita. In particolare, consentono di risalire al posto di lavoro, residenza, luoghi maggiormente frequentati e dati riservati quali religione o preferenze sessuali.
- *Dati che evidenziano crimini oppure violazioni del codice della strada.*

A partire dalla progettazione e per impostazione predefinita, i titolari del trattamento devono configurare le tecnologie impiegate ed offrire impostazioni predefinite affinché la vita privata sia salvaguardata, assicurare che gli interessati ricevano le dovute informazioni, con la facoltà di poter cambiare facilmente le loro configurazioni.

In aggiunta, il conducente deve ricevere le informazioni riguardanti il trattamento nella sua lingua; solamente i dati indispensabili all'operatività del mezzo si devono trattare per impostazione predefinita; agli interessati deve essere concessa la possibilità di abilitare o disabilitare il trattamento per qualsiasi altro scopo ad opera di qualsiasi altro titolare ed inoltre eliminare i dati che non devono essere condivisi con terzi ma che devono essere custoditi soltanto per il tempo opportuno alla fornitura del servizio. Per concludere, i dati devono essere eliminati in maniera definitiva prima che la vettura sia rivenduta.

La ricercatrice *Nynke Elske Vellinga* dell'università di Groningen nei Paesi Bassi ha pubblicato nel 2022 un lavoro nel quale affronta il tema della sicurezza informatica dei veicoli. Più in dettaglio, vengono presentati sei principi relativi alla cybersecurity delle vetture:

1. L'accesso senza autorizzazione ai sistemi del veicolo deve essere ostacolato;
2. Qualora il suddetto accesso abbia luogo, è necessario ridurre al minimo i danni;
3. Qualora il suddetto accesso abbia luogo, si dovrebbe riabilitare lo stato di sicurezza informatica;
4. I soggetti offesi devono ricevere un adeguato risarcimento;
5. Colui che approfitta di una vulnerabilità di sicurezza informatica dovrebbe essere chiamato a rispondere delle proprie azioni in conformità al diritto amministrativo e penale;
6. Lo stato di sicurezza informatica andrebbe difeso durante l'intero ciclo di vita del veicolo.

Il primo principio rappresenta il fulcro della regolamentazione della sicurezza informatica; invece, il secondo introduce uno step successivo qualora il principio 1 non possa essere adempiuto. Le modalità con le quali l'hacker riesce a conseguire l'accesso non sono di particolare importanza. Il secondo principio sottolinea l'importanza di adottare strumenti e misure di regolamentazione al fine di contenere potenziali danni provocati da un hacker e favorire il ripristino dello stato di sicurezza informatica.

Con lo scopo di assicurare un'efficace gestione dei danni, le regolamentazioni di tipo tecnico dovrebbero prevedere delle misure di sicurezza particolari volte a garantire l'isolamento dei sistemi non critici per la sicurezza e dei controlli critici per la sicurezza dell'automobile. Con questo approccio, si costruiscono livelli successivi di protezione configurando una sorta di 'struttura a cipolla' per la cybersecurity. Oltre a ciò, tutti i sistemi del veicolo si potrebbero sviluppare secondo un approccio failsafe, ovvero nel caso in cui la vettura subisca un attacco, essa ritorna ad uno stato di rischio minimo, permettendo di ridurre i danni causati dall'uso di una vulnerabilità. In aggiunta, più velocemente si ripristina lo stato di sicurezza informatica, meno gravi saranno i danni subiti. Per fare questo, la stessa casa automobilistica potrebbe essere chiamata ad intervenire, ad esempio richiamando tutti i veicoli che adoperano lo stesso software presente nella vettura hackerata. Allo stesso tempo, potrebbe essere necessario che un programmatore di software elabori un aggiornamento per risolvere la vulnerabilità presente. Per fare in modo che questo sia possibile, sono necessarie delle

regole per il controllo dello stato di sicurezza informatica dell'auto, procedure di richiamo e obblighi legati agli aggiornamenti del software.

Qualora i precedenti interventi non dovessero bastare e accadesse un danno, entrerà in gioco il quarto principio che sottolinea l'importanza di un risarcimento alle parti lese. Però, se per ottenerlo risulta indispensabile individuare l'hacker, ciò può essere complesso e potrebbe addirittura essere impraticabile. Comunque questo non deve essere visto come una barriera insormontabile poiché altri soggetti potrebbero essere chiamati in causa come responsabili del danno provocato. Nell'eventualità in cui la parte offesa non sia in grado di identificare il colpevole, potrebbe ricevere un risarcimento attraverso un fondo che gestisce questa situazione.

Tanto la responsabilità civile quanto il diritto civile rappresentano delle forme di deterrenza, ma pure la responsabilità penale può agire in tal senso, evidenziando la rilevanza del quinto principio.

Con l'incremento delle innovazioni tecnologiche, cambiano anche le tipologie di minacce alla cybersecurity. Di conseguenza risulta essenziale tenere sotto controllo i veicoli durante tutto il loro ciclo di vita come indicato nel sesto principio. Per fare ciò, sono necessarie attività di monitoraggio e aggiornamento, nelle quali vengano coinvolti i costruttori di automobili, le autorità di omologazione dei veicoli e i proprietari stessi dei veicoli.

A Gennaio 2022 l'Unione Europea ha approvato il *regolamento R155 definito dallo United Nations Economic Commission for Europe (UNECE)*, un organo delle nazioni unite che svolge vari compiti, tra cui quello di stabilire delle norme relative all'omologazione dei veicoli. Questo regolamento è valido da Luglio 2022 per quei veicoli di nuova omologazione, mentre da Luglio 2024 per ogni altro veicolo immatricolato. All'interno dell'R155 sono presenti diversi requisiti riguardanti il veicolo e le sue componenti al fine di assicurare la 'security by design', vale a dire l'integrazione della sicurezza informatica lungo l'intera evoluzione dell'autoveicolo a partire dalla progettazione sino alla rottamazione. Non si tratta di una norma che deve essere rispettata esclusivamente dalle case produttrici di automobili, bensì anche i fornitori devono partecipare attivamente alle fasi di sviluppo di un mezzo di trasporto che sia 'secure by design', implementando un sistema di sorveglianza attiva per identificare rischi e vulnerabilità che potrebbero emergere durante l'utilizzo. Per prima cosa, viene presentata una definizione della sicurezza informatica in ambito automotive: "la condizione in cui i veicoli stradali e le loro funzioni sono protetti da minacce informatiche nei confronti dei componenti elettrici o elettronici". Dalla suddetta definizione risulta evidente come la sicurezza sia una condizione e non un'attività che si può realizzare mediante specifiche attività e processi, in modo tale da difendere i veicoli da potenziali minacce. All'interno della R155 sono presenti due prospettive complementari: da un lato vengono regolamentati i processi utilizzati all'interno dell'impresa per la gestione della Cybersecurity, dall'altro lato si definiscono delle norme sulla cybersecurity in merito al prodotto. Nel primo caso si fa riferimento al Cybersecurity Management System o CSMS, che rappresenta un sistema per la gestione della sicurezza informatica di cui le case automobilistiche devono munirsi. I suoi elementi chiave sono:

- Adottare processi che permettano di individuare, esaminare e mitigare i rischi relativi agli attacchi informatici;

- Dalla progettazione fino al momento in cui il prodotto è operativo presso il cliente si effettua la gestione del rischio;
- Controllo sulle vulnerabilità emergenti e su attacchi cibernetici noti al fine di poter rilasciare nuovi aggiornamenti che li prevengano o li contrastino;
- Questo sistema può essere sottoposto ad una valutazione a opera di un ente di certificazione accreditato.

Per quanto concerne la seconda prospettiva, cioè le norme sulla cybersecurity riguardo al prodotto, vengono elencate delle classi di rischi da tenere in conto, lasciando al produttore di veicoli e ai fornitori la libertà di scegliere tecniche e soluzioni per proteggersi ma stabilendo l'ambito da tener presente.

Al fine di tutelare la sicurezza dell'utente, in aggiunta, il regolamento stabilisce che si debbano individuare le minacce più probabili al sistema e stimare potenziali danni, inclusa la loro entità attraverso il Threat Analysis and Risk Assessment (TARA). Tra i parametri di sicurezza sono inclusi sicurezza stessa, funzionamento dell'automobile, danno economico e privacy dell'utente.

Dato che le vetture di oggi hanno al loro interno una quantità di componenti elettronici e software costantemente in crescita, ciò implica che queste componenti debbano essere sempre aggiornate per assicurare la sicurezza degli utenti. Infatti, negli ultimi tempi si è verificato un continuo susseguirsi di standard di riferimento nella procedura di certificazione per la conformità al regolamento UNECE R155. Uno dei più recenti è l'ISO/SAE-21434 che costituisce un importante avanzamento per il settore automotive, integrando le più moderne innovazioni tecnologiche e risolvendo molte delle problematiche e carenze emerse dai precedenti standard. Non solo, al suo interno è presente un'analisi approfondita della metodologia TARA, utilizzata durante la fase di progettazione di un nuovo prodotto al fine di valutare i rischi per cybersecurity e privacy. Questa valutazione avviene su due rami: da un lato per anticipare la serietà delle minacce, determinando l'impatto potenziale sul prodotto o sul sistema; dall'altro lato per effettuare una stima della probabilità che un attacco si verifichi, tenendo conto dei seguenti fattori chiave:

- tempo di esecuzione – il tempo che un malintenzionato impiegherebbe per dare inizio ad un attacco;
- competenza richiesta – definisce il livello di abilità che deve possedere un malintenzionato;
- familiarità con il componente – rappresenta il grado di conoscenza del malintenzionato nei confronti del bersaglio;
- strumenti necessari – si fa riferimento alle attrezzature indispensabili per lanciare l'attacco.

A proposito di software, visto che in un futuro non troppo lontano i veicoli autonomi probabilmente entreranno a parte dei veicoli in circolazione sulle strade, diventa cruciale gestire adeguatamente il software dell'automobile e aggiornarlo regolarmente. In questo contesto opera il regolamento R156 che dispone l'implementazione e il funzionamento di un sistema di gestione degli aggiornamenti del software (Software Update Management System o SUMS). Questo sistema viene descritto come un metodo strutturato che stabilisce processi e procedure organizzative per adeguarsi ai requisiti relativi alla distribuzione degli aggiornamenti software previsti dal regolamento. Inoltre, sono definiti norme e standard specifici ai quali i mezzi di trasporto devono attenersi con lo scopo di assicurare la

sicurezza degli aggiornamenti software. Più in dettaglio, alle case automobilistiche è richiesto di adottare adeguate misure di sicurezza informatica al fine di mitigare eventuali rischi dovuti agli aggiornamenti software. Le suddette misure comprendono:

- Adottare un SUMS;
- Approvare l'integrità del software per evitare violazioni;
- Conservare dei registri degli aggiornamenti a fini di monitoraggio;
- Introdurre dei meccanismi di controllo degli accessi allo scopo di salvaguardare da accessi non autorizzati;
- Preservare i canali di comunicazione per l'attività di aggiornamento.

Tramite il CSMS e il SUMS si vuole far in modo che i produttori di automobili inseriscano tra gli obiettivi aziendali quello di conseguire uno stato di sicurezza informatica. Pertanto, l'R155 e l'R156 supportano il primo principio precedentemente illustrato, con l'obiettivo di prevenire l'accesso non autorizzato.

Per quanto riguarda il secondo e terzo principio, entrambe le norme manifestano delle lacune. Più nel dettaglio, considerano la possibilità di revocare l'approvazione o il certificato nel caso in cui non siano più rispettati i requisiti previsti da queste regolamentazioni. In tal modo è possibile contenere il danno derivante dall'uso di una vulnerabilità di sicurezza informatica; tuttavia, non sono previsti requisiti per ridurre il danno che può originarsi subito dopo l'attacco informatico. L'R155 stabilisce che un veicolo deve essere capace di rilevare e reagire a potenziali attacchi cibernetici ma non specifica quale debba essere questa reazione.

Riguardo al ripristino dello stato di sicurezza informatica (terzo principio), questo non viene trattato con l'attenzione che meriterebbe. A titolo di esempio, nell'R156 non si specificano i tempi entro cui deve essere rilasciato un aggiornamento software.

Dato che entrambe le norme (R155 e R156) prevedono l'eventualità di revocare ogni omologazione di un veicolo qualora questo non rispetti i requisiti dei regolamenti, si può concludere che il sesto principio è supportato.

In linea generale, le suddette normative danno l'impressione di essere focalizzate soprattutto nell'evitare l'accesso non autorizzato.

Capitolo 5-Guida autonoma

Per quanto riguarda il futuro dei veicoli, uno dei protagonisti sarà sicuramente *la guida autonoma*. Secondo un'indagine condotta dalla National Highway Traffic Safety Administration (NHTSA) degli Stati Uniti, all'incirca il 94% dei sinistri stradali è attribuibile a sbagli commessi dall'uomo. Tra le motivazioni che hanno spinto case automobilistiche, legislatori e funzionari ad introdurre significativi avanzamenti nei sistemi di trasporto sono incluse una cultura stradale inadeguata e un'inosservanza delle norme sottolineata dal precedente dato. In questa direzione, sono in corso un numero sempre maggiore di sforzi di ricerca e sviluppo per incrementare la sicurezza e la capacità di automazione dei mezzi di trasporto a guida autonoma con lo scopo di ridurre gli incidenti stradali e migliorare le infrastrutture stradali. Intel, azienda statunitense che realizza semiconduttori e microprocessori, ha realizzato un report sui vantaggi attesi dei veicoli autonomi, il quale mostra che il loro ingresso sulle strade porterà ad un calo di 250 milioni di ore di mobilità pendolare degli utenti all'anno, oltre che mettere in salvo più di 500 mila vite tra il 2035 e il 2045, soltanto negli Stati Uniti.

Per poter parlare di guida autonoma, è necessario fare un po' di chiarezza sulla definizione e i differenti livelli. I veicoli possono essere dotati di vari livelli di automazione a seconda delle tecnologie integrate e delle capacità intelligenti. La *Society of Automotive Engineers International*, un'organizzazione globale che riunisce ingegneri, tecnici e scienziati con lo scopo di stabilire norme e standard per il settore aerospaziale e automotive, ha definito sei livelli di guida autonoma:

- Livello 0 – *Nessuna automazione*, ciò vuol dire che l'unico responsabile di comportamenti scorretti alla guida sarà il conducente umano;
- Livello 1 – *Assistenza alla guida* tramite la presenza di un supporto di guida automatizzato per alcune funzioni come acceleratore, frenata o sterzo, però la responsabilità di altre eventuali operazioni di guida resta al conducente;
- Livello 2 – *Automazione parziale* che prevede la disponibilità dei sistemi avanzati di assistenza alla guida (ADAS);
- Livello 3 – *Automazione condizionale* e in questo caso il veicolo presenta funzionalità maggiormente avanzate;
- Livello 4 – *Elevata automazione* con la quale una vettura è in grado di compiere tutte le operazioni di guida all'interno di un'area georeferenziata alcune aree;
- Livello 5 – *Automazione completa* significa che un mezzo di trasporto può compiere ogni tipo di operazione di guida.

La seguente immagine illustra i 6 livelli di autonomia con ulteriori precisazioni.



Fig.9 – Fonte: https://www.alvolante.it/da_sapere/tecnologia/5-livelli-della-guida-autonoma-396147

Ad oggi, le vetture circolanti sulle strade italiane possono essere dotate al massimo del livello 2 e ciò significa che acceleratore, sterzo e freni possono essere controllati dall'elettronica ma dato che non è in grado di farlo in ogni situazione, il guidatore deve tenere le mani sul volante. Passando al livello successivo (3), non ci sono grossi cambiamenti se non il fatto che entro i limiti imposti dall'elettronica, il conducente può distogliere lo sguardo dalla strada e togliere le mani dal volante. Tuttavia, è necessario rimanere sempre pronti a intervenire e riprendere il comando all'occorrenza. In Italia il livello 3 non è consentito dalla legge, mentre paesi come Regno Unito e Germania lo hanno regolamentato e sono già disponibili sul mercato veicoli dotati di queste funzionalità, come alcuni modelli della Mercedes.

Una volta considerata pura fantascienza, la guida autonoma risulta ormai una realtà in rapida diffusione anche grazie al contributo dell'*intelligenza artificiale (IA)*. Pure quest'ultima, come d'altronde ogni tecnologia, si sviluppa attraverso un continuo processo di apprendimento al fine di migliorarne funzionalità e potenzialità. In ottica di guida autonoma, ciò si concretizza in sofisticati algoritmi di autoapprendimento, formati da livelli sovrapposti, sottoinsiemi e nodi che costituiscono un'ampia rete neurale. In merito a questo tema, la difficoltà maggiore consiste nell'istruire tale 'cervello artificiale' al fine di renderlo in grado di distinguere le varie situazioni di traffico nelle quali si potrebbe trovare e successivamente mettere in atto una reazione apposita per ciascuna. A titolo di esempio: le vetture in coda, impedimenti imprevisti e riconoscere l'aspetto di oggetti e persone nelle diverse stagioni. Di conseguenza, tanto l'esperienza quanto l'acquisizione di dati in movimento assumono un ruolo fondamentale per la raccolta di dati empirici al fine di consentire agli algoritmi di apprendere ed adattarsi alle reali complessità del traffico. Chiaramente, i colossi come ad esempio Google possono godere di una notevole superiorità in questo processo tramite gli svariati anni di sperimentazioni su strada, che hanno dato origine a database inestimabili, i quali saranno fondamentali per rendere l'IA adeguata a gestire la guida autonoma. Infatti, l'azienda che ad oggi risulta essere leader nel servizio dei Robotaxi negli Stati Uniti è la Waymo, di proprietà di Alphabet, che ad oggi può vantare la presenza di ben 800 veicoli autonomi operativi in California e Phoenix. Nei prossimi anni ci sarà un aumento dell'utilizzo, dell'efficienza e dell'efficacia dell'IA nella vita

quotidiana a bordo delle vetture. In particolare, saranno le interazioni tra veicoli ed infrastrutture a beneficiarne, favorendo un miglioramento degli spostamenti delle auto a guida autonoma.

L'IA combinata con l'uso di algoritmi di deep learning ha portato significativi progressi su diversi elementi fondamentali della tecnologia per la guida autonoma. Non a caso, con l'evoluzione dei sistemi di guida supportati dall'IA, il numero di veicoli autonomi sulle strade è cresciuto notevolmente negli ultimi 10 anni in diversi paesi sviluppati d'Europa, così come negli Stati Uniti e in Canada. Nonostante ciò, questa tipologia di veicoli ha provocato vari incidenti stradali generando scetticismo nell'opinione pubblica e spingendo numerosi studi ad evidenziare le correnti limitazioni e criticità relative a progettazione, sviluppo e implementazione. Burton et al. hanno pubblicato un documento nel quale illustrano 3 problemi ancora irrisolti riguardanti lo sviluppo all'avanguardia dei sistemi autonomi. Il *divario semantico* è il primo e corrisponde alla differenza tra funzionalità previste e quelle specificate, ovvero le intenzioni implicite e ambigue del sistema risultano essere maggiormente differenti in confronto alle specifiche esplicite e concrete del sistema. Il secondo è il *divario di responsabilità in termini morali* che emerge ogni qual volta si verifica un incidente stradale e non si riesce a stabilire se la responsabilità sia del conducente o del sistema autonomo. Individuare chi si possa ritenere moralmente responsabile per danni e lesioni causati dalla condotta del sistema sarà verosimilmente una condizione essenziale per poter guadagnare la fiducia pubblica nei sistemi autonomi. Infine, il terzo ed ultimo è il *divario di responsabilità civile* che pone il problema di chi debba farsi carico del risarcimento dei feriti in caso di incidente dato che i sistemi o i prodotti non hanno personalità giuridica e ciò implica che non sono vincolati da diritti o doveri legali.

Le criticità e i timori nei confronti dell'IA hanno spinto le istituzioni a elaborare quadri legislativi con lo scopo di controllare le attività dei sistemi basati sui dati tanto su scala nazionale quanto su quella internazionale. L'UE ha recentemente pubblicato delle *linee guida etiche per un'intelligenza artificiale affidabile*, le quali propongono *sette requisiti essenziali* che devono essere rispettati dai sistemi di IA per poter essere ritenuti affidabili. I requisiti sono 1) intervento e sorveglianza umani, 2) robustezza tecnica e sicurezza, 3) riservatezza e governance dei dati, 4) trasparenza, 5) diversità, non discriminazione ed equità, 6) benessere sociale e ambientale, 7) accountability.

La nota azienda di servizi di consulenza *McKinsey & Company*, ha realizzato un *report riguardante gli scenari futuri della guida autonoma sui veicoli privati*. Di seguito verranno illustrati risultati e conclusioni.

Le vetture autonome potrebbero trasformare in maniera radicale l'esperienza dei consumatori nel campo della mobilità, facendo diventare gli spostamenti in auto maggiormente sicuri, confortevoli e piacevoli. Il tempo che prima veniva dedicato esclusivamente alla guida, si potrebbe sfruttare per videochiamate con amici, guardare un film oppure dedicarsi al lavoro. Nel caso di dipendenti che percorrono lunghe distanze tra casa e ufficio, viaggiare su un veicolo autonomo potrebbe incrementare la produttività e contribuire alla riduzione della giornata lavorativa. Di conseguenza, risulterebbe più semplice vivere lontano dall'ufficio e può darsi che un numero crescente di persone si trasferisca in zone rurali e nelle periferie. Inoltre, anche gli anziani ne trarrebbero benefici, poiché nel loro caso la guida autonoma rappresenterebbe un'alternativa di mobilità che supera i limiti dei trasporti pubblici e dei servizi di car sharing. Non solo, pure la sicurezza verrebbe ottimizzata come

illustrato in uno studio che mostra l'impatto positivo della crescente diffusione degli ADAS che ridurrebbe del 15% il numero di sinistri entro il 2030.

Sulla base di un sondaggio effettuato nel 2021 sempre dalla McKinsey&Company, i consumatori mostrano particolare interesse per le funzionalità di guida autonoma e disponibilità a pagarle. Tenendo conto di questo interesse e di quello mostrano nei confronti delle soluzioni commerciali presenti sul mercato, le stime prevedono un flusso economico generato da ADAS e sistemi di guida autonoma che si aggira tra 300 e 400 miliardi di dollari entro il 2035, come illustrato dalla seguente immagine.

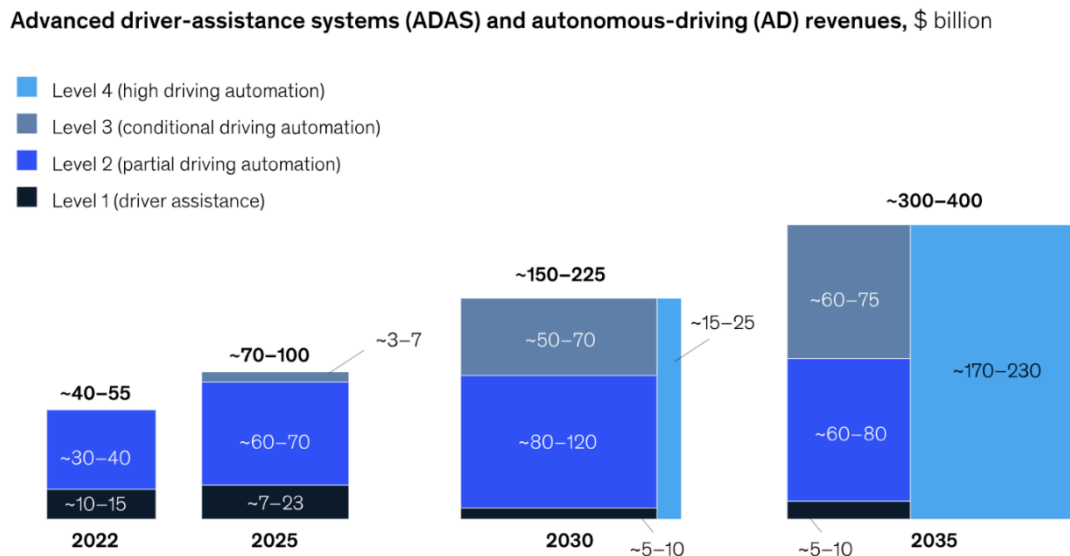


Fig.10 – Fonte: “Autonomous driving’s future: Convenient and connected” di McKinsey & Company

Le ripercussioni delle auto a guida autonoma su altri settori potrebbero essere rilevanti. Per esempio, i conducenti magari non dovranno più sostenere il costo di elevati premi assicurativi, perché affidando il controllo della vettura al sistema di guida autonoma, la responsabilità in caso di incidente potrebbe non ricadere più sull'essere umano. Pertanto, nuovi modelli assicurativi B2B dedicati a questa categoria di veicoli potrebbero nascere. Sono diverse le aziende automobilistiche che hanno già avviato sperimentazioni su soluzioni assicurative innovative. Tramite la tecnologia autonoma, raccolgono dati sullo stile di guida del conducente per sviluppare proposte su misura per i loro clienti. Grazie al controllo che gli OEM esercitano sul sistema di guida autonoma, le sue performance e i dati che produce, le case automobilistiche sono in grado di adattare con accuratezza le polizze assicurative alle esigenze dei consumatori, garantendosi così un notevole vantaggio in confronto alle compagnie assicurative.

Alla luce degli elevati livelli di incertezza che stanno caratterizzando il settore dell'automotive, McKinsey ha elaborato *tre scenari* per le vendite di veicoli autonomi, tenendo in considerazione vari livelli di disponibilità della tecnologia, adozione da parte dei clienti, e sostegno proveniente dalle normative.

Nello scenario *Delayed*, le tempistiche di introduzione sul mercato delle autovetture autonome da parte delle case automobilistiche vengono ulteriormente posticipate, mentre l'adozione da parte dei

consumatori resta limitata. Si stima che entro il 2030, la percentuale di vetture vendute con dotazione di guida autonoma di livello 3 o superiore sarà pari solamente al 4%, ma nei successivi cinque anni (2035) salirà al 17%.

Estimated passenger vehicles sold with autonomous-driving technologies installed, %

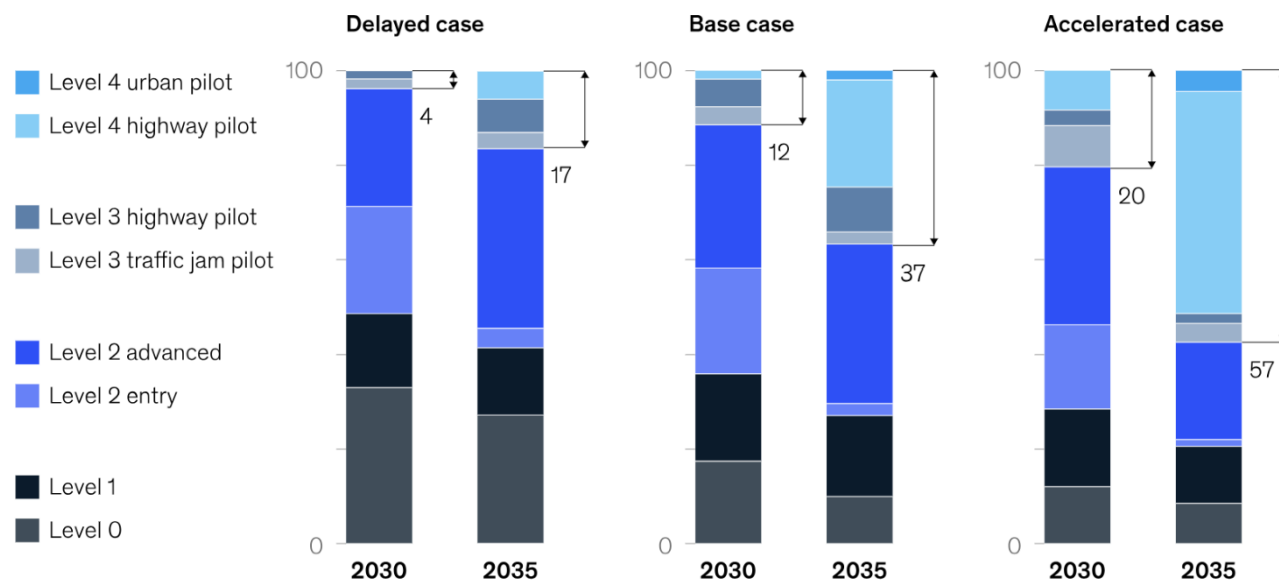


Fig.11 – Fonte: “Autonomous driving’s future: Convenient and connected” di McKinsey & Company

Per quanto riguarda lo scenario *Base*, si ipotizza che gli OEM riescano ad attenersi alle tempistiche dichiarate per il lancio dei veicoli autonomi e che ci sia un livello medio di adozione da parte dei consumatori. Le stime mostrano che prima della fine del 2030, la quota percentuale di vetture vendute con tecnologie autonome di livello 3 o superiore sarà del 12%, per poi triplicare (37%) nel 2035.

Per concludere, il terzo ed ultimo scenario è quello *Accelerated*, nel quale gli OEM introducono in maniera rapida i veicoli autonomi nel mercato, generando significativi ricavi grazie a modelli di business innovativi. Buona parte delle case automobilistiche di fascia alta effettua installazioni predefinite di hardware attraverso il quale la guida autonoma può essere attivata effettuando un banale aggiornamento del software. Da un punto di vista quantitativo, il 20% delle auto vendute sarà equipaggiato con livelli di guida autonoma pari a 3 o superiore entro il 2030, mentre saliranno al 57% entro il 2035.

Basandosi sulle suddette stime, si può ipotizzare un notevole potenziale di crescita per tutte quelle aziende produttrici di auto che sono particolarmente orientate sulla produzione di vetture con livelli di automazione elevati. I consumatori potrebbero essere attratti dai veicoli con funzioni autonome più avanzate come nel caso di livello 3 e 4, in quanto rendono più confortevole la guida. Non solo, sensori e computer ad elevate prestazioni hanno costi in continua riduzione e allo stesso tempo, gli standard di sicurezza relativi alle tecnologie di guida autonoma fanno costanti progressi.

Secondo le previsioni di vendita di McKinsey, saranno i sistemi di guida autonoma di livello 3 e 4 specifici per l’autostrada, quelli ampiamente disponibili in Europa e Nord America entro il 2025 per il segmento delle automobili private.

Data la presenza di alti costi iniziali per la realizzazione di sistemi di guida L3 ed L4, le case automobilistiche potrebbero inizialmente focalizzare i loro sforzi per la vendita di sistemi di guida autonoma maggiormente sofisticati, sui segmenti di vetture di fascia alta. Le licenze hardware e software per ciascun veicolo dotato di sistemi L3 ed L4, potrebbero generare oneri supplementari pari o superiori a 5000\$ nel periodo iniziale di lancio, mentre le spese per sviluppo e approvazione è presumibile che eccedano il miliardo di dollari. Di conseguenza il prezzo di vendita per questi veicoli verosimilmente raggiungerà valori notevoli; quindi, potrebbe risultare più conveniente dal punto di vista commerciale puntare sull'offerta di sistemi L2.

Ad oggi, sono diversi gli OEM che offrono vetture equipaggiate con sistemi L2, anche grazie all'introduzione di nuove norme come il regolamento 2019/2144, che incrementa il numero di ADAS che le automobili devono avere a bordo. Infatti, sia l'industria automobilistica che le autorità pubbliche sono d'accordo sul fatto che la guida autonoma possa avere un impatto significativo nel salvare vite.

Un altro documento molto interessante è un *sondaggio realizzato dal McKinsey Mobility Consumer Pulse che analizza in maniera periodica le percezioni e le preferenze su mobilità futura e guida autonoma*. In particolare, si tratta di un sondaggio realizzato nel Dicembre 2022, coinvolgendo 30.978 utenti attuali della mobilità di 15 mercati tra cui Emirati Arabi Uniti, Francia, Stati Uniti, Corea del Sud, Giappone, Regno Unito, Brasile, Norvegia, Cina, Italia, Sudafrica, Egitto, Australia, Arabia Saudita e Germania. Di seguito le relative conclusioni.

Oltre la metà degli automobilisti (51%), prevede di cambiare in futuro la propria auto con un veicolo completamente autonomo. Di questo gruppo, il 19% è disposto a passare ad un veicolo a guida autonoma che non preveda la possibilità di guida manuale, mentre il 32% effettuerebbe il cambio esclusivamente se rimanesse a bordo l'opzione di guida manuale. Per quanto riguarda gli ostacoli nei confronti della scelta di un veicolo autonomo, i consumatori hanno evidenziato che la loro principale preoccupazione riguarda la sicurezza, ma non solo, ritengono indispensabile avere più informazioni e testare questa tecnologia in prima persona al fine di dare origine ad una maggiore fiducia.

Relativamente all'uso di ADAS di base come cruise control e assistenza al parcheggio, in media, tra il 25 e il 30% degli automobilisti che guidano auto equipaggiate con i suddetti supporti alla guida, afferma di utilizzarli raramente oppure mai. Le motivazioni predominanti spaziano dal piacere di guidare alla mancanza di chiarezza sul quando utilizzarli, fino alla paura per un possibile malfunzionamento della tecnologia.

Il 50% dei consumatori che sono inclini o altamente motivati ad acquistare una funzione di guida autonoma di livello 4, si dichiarano pronti a sostenere il pagamento di un premio una tantum del valore di 9.999\$ per poterla acquisire.

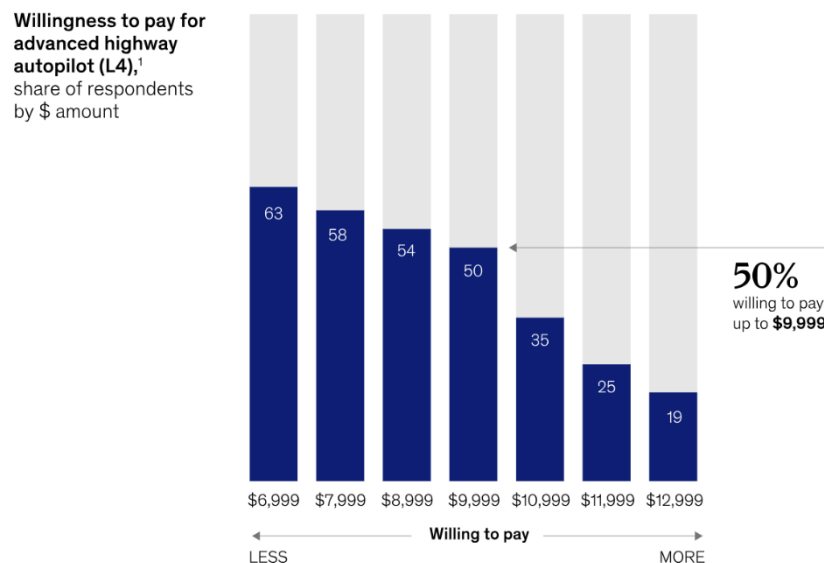


Fig.12 – “Hands off: Consumer perceptions of advanced driver assistance systems” di McKinsey & Company

La maggioranza dei consumatori privilegia l’acquisizione degli ADAS come elemento integrante della configurazione totale della vettura oppure come aggiornamenti successivi all’acquisto, pagando un prezzo fisso per lo specifico ADAS che si vuole aggiungere. Nonostante ciò, il 23% mostra una preferenza per schemi di abbonamento flessibili oppure soluzioni pay-per-use attivabili su richiesta. Tutto sommato, i consumatori esprimono un elevato appagamento nei confronti della loro esperienza con i sistemi ADAS presenti a bordo delle loro automobili. Poco meno dell’80% sarebbe disposto a riacquistare le funzionalità ADAS presenti nel suo veicolo e quasi uno su 3 di loro chiederebbe uno sconto basandosi sulla propria esperienza.

Gli ADAS sembrano anche rappresentare una discriminante nella scelta del marchio automobilistico, specialmente tra coloro che acquistano veicoli elettrici e quelli del segmento dei brand premium. Il 42% dei compratori di mezzi di trasporto elettrici e il 38% degli acquirenti di vetture di marchi premium dichiarano di essere fortemente inclini a scegliere un’altra casa automobilistica per ottenere caratteristiche ADAS superiori. Tra quei consumatori che comprano veicoli con motore a combustione interna, soltanto il 22% dichiara di essere altamente propenso a cambiare marchio.

Likelihood of switching car brands for better advanced driver-assistance systems (ADAS),
 % of respondents who are interested in buying a new car

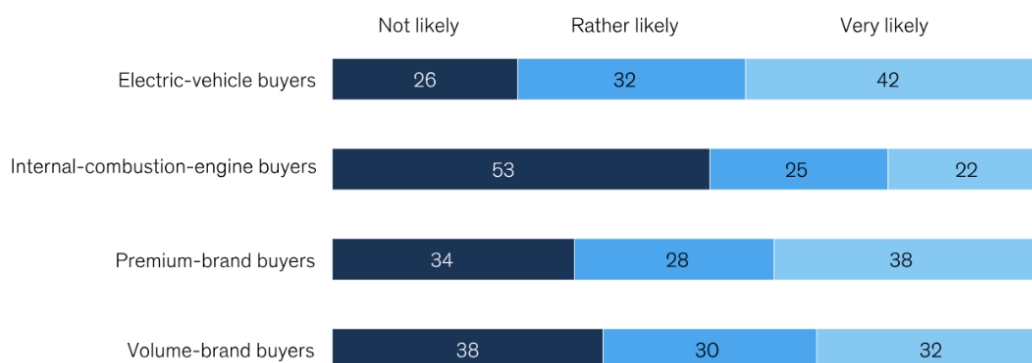


Fig.13 – Fonte: “Hands off: Consumer perceptions of advanced driver assistance systems” di McKinsey & Company

Inoltre, i consumatori mostrano una crescente inclinazione verso l’adozione di funzionalità di guida autonoma di livello L2 o L3 nei loro veicoli privati, ma allo stesso tempo manifestano maggiore interesse per le funzionalità L4 o L5 nell’ambito della mobilità condivisa. All’incirca il 50% abbandonerebbe del tutto l’uso della propria auto nel caso in cui i servizi di veicoli autonomi condivisi fossero a disposizione nella loro città di residenza, mentre l’81% è favorevole alla possibilità di condividere una navetta autonoma.

Le tecnologie di guida autonoma possiedono un immenso potenziale per incrementare la sicurezza e il comfort dei conducenti, creare un notevole valore nel settore dell’automotive e rivoluzionare la mobilità delle persone. Tuttavia, il mercato delle vetture a guida autonoma risulta dinamico ed in continua evoluzione, generando elevati livelli di incertezza.

Capitolo 6-Prospettive future

La strategia europea sui dati, introdotta nel 2020, delinea l'obiettivo dell'Europa di affermarsi come leader mondiale nella data-agile economy, fungendo anche da modello di riferimento per una società che utilizza i dati per migliorare i processi decisionali sia in ambito industriale che governativo. Lo "European Data Market Study 2021-2023" mostra delle previsioni per il futuro dell'economia e del mercato europeo dei dati attraverso l'elaborazione di tre scenari alternativi che valutano la combinazione di fattori e decisioni politiche che possono contribuire al conseguimento degli ambiziosi obiettivi dell'UE oppure, diversamente, causare un rallentamento. I suddetti tre possibili scenari sono i seguenti.

Baseline Scenario, nel quale le principali ipotesi si fondano sul proseguimento delle attuali tendenze di crescita ed evoluzione delle attuali condizioni quadro o framework. Queste ultime rappresentano una moltitudine di fattori istituzionali, informativi e socioeconomici che caratterizzano il contesto locale e tipicamente includono i seguenti ambiti: normative, supporto, accesso ai finanziamenti, condizioni di mercato, cultura e creazione di conoscenza. A causa degli elevati tassi di interesse e delle tensioni commerciali, la crescita economica dell'UE subirà un rallentamento, con tassi di crescita del PIL contenuti fino al 2025 e una ripresa graduale a partire dal 2026. Questo scenario si distingue per una moderata concentrazione di potere tra i colossi che possiedono gran parte dei dati in circolazione, un sistema di governance dei dati che tutela i diritti degli individui e una distribuzione disomogenea ma allo stesso tempo relativamente ampia dei benefici derivanti dall'innovazione dei dati tra i diversi paesi e all'interno della società.

High Growth Scenario, prevede una crescita più rapida per il mercato dei dati, favorita da un contesto generale più stabile. Per fare in modo che ciò sia possibile, si dovrebbe verificare un miglioramento delle condizioni geopolitiche, con il contenimento delle minacce di escalation bellica nel Medio Oriente, l'instaurazione di un cessate il fuoco nel conflitto tra Israele e Gaza, tra Russia e Ucraina, l'assenza di azioni aggressive nei confronti di Taiwan da parte della Cina e una presidenza statunitense che adotti una politica estera equilibrata e stabile. Se le precedenti supposizioni si avverassero, allora le tensioni commerciali globali e le pressioni inflazionistiche sui prezzi dell'energia e delle materie prime si ridurrebbero. Inoltre, se l'inflazione fosse riportata sotto controllo entro il 2025, attraverso una politica monetaria più rilassata si potrebbe favorire un ciclo di crescita economica più sostenuto per i prossimi cinque anni. Un miglioramento delle condizioni economiche come precedentemente descritto, comporterebbe un'adozione più veloce dell'innovazione dei dati in confronto alla scenario baseline, all'interno di un contesto di condivisione dei dati adeguatamente sostenuto da un sistema di governance dei dati e da politiche industriali di successo in Europa.

Challenge Scenario potrebbe emergere a causa di sviluppi negativi in alcune delle attuali crisi geopolitiche. In questo contesto, le condizioni del commercio internazionale si deteriorerebbero, provocando un incremento della pressione sui prezzi dell'energia e delle materie prime, con il rischio di frenare la transizione green a causa della riduzione delle esportazioni di materiali essenziali, ad esempio per la realizzazione di pannelli solari, impianti eolici o batterie. Tutto questo comporterebbe il manifestarsi di uno scenario di stagflazione caratterizzato da crescita bassa o nulla del PIL ed un incremento dei prezzi medi di beni e servizi. Contemporaneamente, le industrie militari e

manifatturiere potrebbero beneficiare di maggiori investimenti e ricavi dovuti ad una crescita della spesa militare. Di conseguenza, l'innovazione guidata dai dati si realizzerebbe ma in maniera disomogenea, concentrandosi principalmente sui mercati governativi e della difesa, anziché sui servizi destinati alle imprese e ai consumatori.

La quota percentuale della monetizzazione dei dati all'interno del mercato dei dati europeo è in continua crescita e secondo le previsioni potrebbe arrivare a toccare entro il 2030 il 36% che corrisponde a 42 miliardi di euro. La crescita della monetizzazione procede a rilento e questo è dovuto al fatto che le aziende stanno ancora scoprendo il potenziale dei dati così come anche il loro valore e le modalità per monetizzarli.

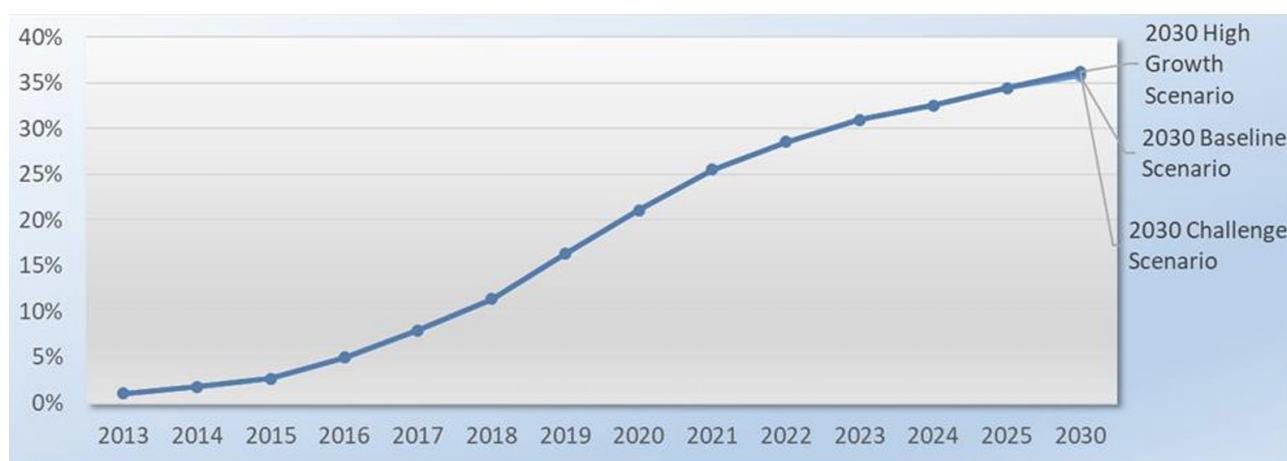


Fig.14 - Quota di monetizzazione dei dati del mercato europeo dei dati 2013-2030 (tre scenari) (%)
– Fonte: European Data Market Study 2021-2023

Relativamente alle previsioni sul mercato dei dati, quest'ultimo arriverà ad un valore di poco superiore ai 118 miliardi di euro considerando il baseline scenario. Nell'orizzonte temporale tra il 2025 e il 2030, corrisponde ad un tasso di crescita annuo composto del 3,3%. Mentre Norvegia, Liechtenstein e Islanda registreranno un incremento maggiore con un tasso di crescita composto del 5,7%, anche se il loro mercato continuerà ad essere una parte ridotta rispetto a quello europeo.

	2025	2030 Challenge Scenario	2030 Baseline Scenario	2030 High Growth Scenario	CAGR: 2020– 2025	CAGR: 2025– 2030, Challenge	CAGR: 2025– 2030, Baseline	CAGR: 2025– 2030, High Growth
EU27	100,212	103,677	118,112	141,025	10.6%	0.7%	3.3%	7.1%
EEA (NO, LI, IS) + CH	3,708	3,808	4,881	6,477	6.4%	0.5%	5.7%	11.8%
Total, All Countries	139,893	144,615	163,063	192,947	7.3%	0.7%	3.1%	6.6%

Fig.15 - Previsioni del mercato dei dati: 2025 (€ '000), tre scenari 2030 (€ '000), e Crescita Composta (%) – Fonte: European Data Market Study 2021-2023

Per quanto riguarda i singoli paesi membri dell'unione europea, il mercato più ampio continuerà ad essere quello della Germania, la cui quota sarà pari al 25% del mercato europeo. La motivazione

risiede nel fatto che le industrie tedesche pongono i dati al centro delle loro strategie e di conseguenza generano un'elevata domanda di dati, strumenti e tecnologie relativi ad essi. Nonostante ciò, la crescita del mercato tedesco sarà inferiore alla media degli altri paesi dell'UE in quanto la maggior parte è già avvenuta proprio per il preesistente focus sui dati da parte delle industrie tedesche.

Riguardo all'economia dei dati, le stime mostrano un valore superiore agli 851 miliardi di euro nel 2030 e un CAGR del 5,3% tra 2025 e 2030, ipotizzando che si verifichi lo scenario baseline. I valori aumentano se si considerano anche quei paesi che si trovano in Europa ma non fanno parte dell'Unione Europea. In dettaglio, aggiungendo il Regno Unito il valore sale a 1110 miliardi di euro, mentre includendo Svizzera e i paesi membri dell'European Economic Area o EEA (Norvegia, Liechtenstein e Islanda), si arriverebbe a 1290 miliardi di euro e un CAGR del 5,4% tra 2025 e 2030.

I	Market	Name	Description	2030 Challenge Scenario	2030 Baseline Scenario	2030 High Growth Scenario	25-30 CAGR			Impacts on GDP		
							2030 Challenge Scenario	2030 Baseline Scenario	2030 High Growth Scenario	2030 Challenge Scenario	2030 Baseline Scenario	2030 High Growth Scenario
5.1 5.2	EU27	Value of the data economy and impacts on EU GDP	Value of total impacts on the EU economy and % of EU GDP	723,421	851,490	994,949	1.9%	5.3%	8.6%	5.2%	5.8%	6.5%
5.1 5.2	EU27+UK	Value of the data economy and impacts on EU GDP	Value of total impacts on the EU economy and % of EU GDP	946,614	1,110,978	1,289,462	2.0%	5.3%	8.5%	5.8%	6.5%	7.2%
5.1 5.2	Total, all countries	Value of the data economy and impacts on EU GDP	Value of total impacts on the EU economy and % of EU GDP	1,024,897	1,204,753	1,396,180	2.0%	5.4%	8.5%	5.9%	6.6%	7.3%

Fig.16 - Valore della Data Economy (€M); 2030 Challenge, Baseline and High Growth Scenarios (€M); Impatto sul Gross Domestic Product (GDP) - Fonte: European Data Market Study 2021-2023

Per quanto riguarda lo scenario Challenge, si prevede una crescita meno rapida per gli impatti sull'economia in generale nel 2030, che oltre ad essere dovuto ad un incremento più moderato del PIL, è influenzato da impatti ridotti che hanno dato luogo a restrizioni più severe nei confronti dell'utilizzo dei dati. Di conseguenza si tratterebbe di uno scenario caratterizzato da ostacoli alla

diffusione capillare e un'intelligenza artificiale che incide in maniera negativa su privacy e adozione in seguito all'emergere di comportamenti pericolosi, tra cui misure di sicurezza insufficienti, alterazione malevola dei dati, generazione di esiti falsati e un utilizzo non disciplinato dei dati.

Di seguito si analizzano in maniera più ampia i tre suddetti scenari.

Per quanto riguarda lo *scenario Baseline*, si stima una crescita media cumulativa del PIL pari a +1,6% tra 2025 e 2030 ed un incremento della spesa ICT del 4,4%, in confronto ad una crescita praticamente piatta nello scenario Challenge. Le previsioni descrivono un'industria europea dei dati in salute, con un continuo progresso nella disponibilità di prodotti e servizi di dati ed una crescita graduale della domanda. L'impatto economico delle recenti normative europee come Digital Markets Act, Data Act e Data Governance Act, contribuisce allo sviluppo di un sistema di governance dei dati riconosciuto su scala globale e che promuove concorrenza e condivisione dei dati, salvaguardando al tempo stesso i diritti degli individui ed evitando che un numero limitato di attori chiave detenga un forte potere sui dati.

Come già detto in precedenza, il mercato dei dati arriverà ad un valore economico pari a 118 miliardi di euro prima della fine del 2030, registrando un CAGR del 3,3%. In maniera progressiva, si prevede la comparsa di un robusto ecosistema dei dati incentrato su varie piattaforme orizzontali e verticali di dati personali e non, che rappresentino un luogo dove poter condividere, acquistare e vendere dati in sicurezza. Tutto questo sarà possibile attraverso la realizzazione degli European Data Spaces per i settori chiave.

Un forte contributo alla crescita del mercato dei dati arriverà da una spinta decisiva sulla transizione green e quella digitale. Attraverso il programma Next-Generation EU, è stato introdotto un meccanismo di recupero straordinario temporaneo dal valore di 750 miliardi di euro allo scopo di agevolare i governi nel porre rimedio ai danni economici e sociali provocati dalla pandemia.

Attraverso investimenti stabili e una stretta cooperazione tra i paesi membri, si favorisce la nascita di infrastrutture di dati autonome e risorse digitali, contribuendo a modellare le norme globali sulla governance digitale in linea con i principi dell'Unione Europea.

Da un lato il futuro regolamento Chips Act mira a promuovere investimenti all'interno degli stabilimenti di produzione dei microprocessori, invece dall'altro l'incremento degli investimenti per la sicurezza informatica ad opera del Digital Europe Programme e la cooperazione a livello nazionale contribuiranno a rafforzare la fiducia e garantire l'utilizzo sicuro di prodotti e servizi ad alta capacità di elaborazione dati.

Per sostenere la ricerca e l'innovazione ed arricchire gli investimenti privati, ci saranno gli investimenti significativi previsti dall'Horizon Europe Programme e Digital Europe Programme.

Come riportato sopra, l'economia dei dati raggiungerà un valore di 851 miliardi di euro entro il 2030, equivalente al 5,8% del PIL totale dei 27 paesi membri. Quindi nello scenario baseline, attraverso la presenza di un florido mercato unico dei dati, l'Europa sarà ben avviata a contribuire all'economia globale dei dati in misura proporzionale al suo peso economico.

Le tecnologie digitali sono adottate con maggiore frequenza da parte di governi e organizzazioni come strumento per promuovere la sostenibilità economica e sociale. Un ruolo cruciale è giocato dagli utenti e dai fornitori IT per la creazione e la messa a punto di asset, processi e operazioni digitali, con l'obiettivo di supportare le organizzazioni a intraprendere pratiche più sostenibili e orientarsi verso un modello di economia circolare, definito come “un modello di produzione e consumo che implica condivisione, prestito, riutilizzo, riparazione, ricondizionamento e riciclo dei materiali e prodotti esistenti il più a lungo possibile.”

In riferimento agli obiettivi di sostenibilità dell'UE, un notevole risultato verrà conseguito per un'ICT ecologica che azzeri l'impatto ambientale dei data center prima della fine del 2030. Da parte dei provider di servizi cloud, verrebbero implementati dei data center maggiormente sostenibili, caratterizzati da un'alta efficienza energetica, impiegando fonti di energia rinnovabili, recuperando il calore di scarto e adottando pratiche circolari per il riciclo e il riutilizzo dei server obsoleti. Per di più, si sta verificando un rapido incremento degli investimenti europei su proposte digitali per gli ambienti di lavoro. Per incentivare la transizione verso un modello di lavoro ibrido, sarà necessario che gli uffici garantiscano la presenza di un ambiente collaborativo capace di promuovere una cultura del lavoro flessibile ma che al tempo stesso preservi la produttività.

Passando allo *scenario High Growth*, i risultati mostrano una crescita più rapida dell'economia europea in confronto allo scenario baseline, con un CAGR pari al 2,6% tra 2025 e 2030, un'accentuata esaltazione dell'innovazione digitale e un aumento significativo degli investimenti totali in ICT del valore di +6,9% tra 2025 e 2030. Non solo, il suddetto scenario si distingue per un progresso significativo nell'innovazione legata ai dati, una diffusa trasformazione digitale a livello europeo, un data framework riconosciuto su scala globale e una minore dipendenza dalla produzione cinese entro il 2030. Inoltre, si prevede un impatto positivo derivante da investimenti specifici per ripristinare i punti di forza dell'Europa nelle aree degli Important Progetti di Comune Interesse Europeo, tra cui semiconduttori, batterie e idrogeno. Questi ultimi, sono dei progetti che si concentrano su fallimenti sistemici o del mercato e sfide condivise legate alla crescita sostenibile e alla competitività dell'economia a livello nazionale e europeo. Per affrontare tali questioni, è fondamentale un coinvolgimento rilevante degli enti pubblici al fine di incentivare le iniziative, fornire supporto economico alla realizzazione e al conseguimento dei relativi obiettivi, favorendo al contempo un maggiore impatto industriale e tecnologico sul sistema produttivo. Attraverso l'efficace messa in opera sull'intera Europa delle politiche della strategia europea sui dati e sul digitale, il loro impatto positivo è massimizzato.

Da un punto di vista quantitativo, le stime mostrano che il mercato dei dati toccherà i 141 miliardi di euro entro il 2030, con un CAGR del 7,1% a partire dal 2025. Le previsioni segnalano che l'economia dei dati raggiungerà un valore pari a 995 miliardi entro il 2030 e ciò costituirà il 6,5% del PIL dell'UE, registrando un CAGR dell'8,6%. In questo contesto, l'economia si tramuterà in un mercato emergente orientato al digitale, in cui più della metà del PIL sarà trainata da prodotti e servizi di aziende trasformate digitalmente.

Il mercato dei dati continuerà a crescere sempre più rapidamente ed allo stesso tempo la tecnologia dei dati si diffonderà ampiamente, raggiungendo un pubblico più vasto di utenti. Supponendo il raggiungimento dell'obiettivo fissato nella strategia dei dati, prima della fine del 2030 si realizzerà

un contesto di policy attraente, al cui interno la quota dell'UE nell'economia dei dati sarà proporzionata al suo peso economico. Mentre all'inizio le dinamiche di domanda e offerta saranno guidate dalla tecnologia, la domanda rappresenterà il driver futuro attraverso la presenza di un ecosistema completamente formato, il quale produrrà cicli di feedback positivi tra imprese di dati e utenti. Si tratta di un tipico processo di circolo virtuoso che si potrebbe manifestare nel caso in cui l'adozione della tecnologia dei dati incrementasse abbastanza rapidamente da generare uno slancio. Non solo, una celere diffusione accresce i benefici per gli utenti nelle loro interazioni e rende più semplice il rafforzamento degli standard e l'interoperabilità, riducendo ancor di più le barriere all'adozione.

Per fare in modo che questo scenario sia possibile, è necessario ipotizzare una sequenza di condizioni di contesto favorevoli. Innanzitutto, attraverso il Data Governance Act si possono riutilizzare i dati posseduti dal settore pubblico. Mentre il Data Act illustra i diritti di proprietà e portabilità dei dati, promuovendo l'emergere di nuovi servizi digitali e l'ingresso di nuovi attori nell'economia dei dati. Infine, con l'applicazione del Digital Markets Act, la supremazia delle Big Tech è parzialmente diminuita grazie agli attori europei in arrivo.

Nel caso in cui tutte le policies e le normative saranno messe in atto e la Commissione sarà in grado di conseguire i traguardi del Decennio Digitale 2030, sarà verosimile un ritmo ottimale di trasformazione digitale e di adozione di tecnologie come 5G, IoT, cloud, 6G e non solo.

Il progredire degli European Data Spaces e l'adozione delle tecnologie big data coinvolgono anche gli utenti comuni oltrepassando i pionieri. Un ecosistema di dati pienamente sviluppato favorisce un ciclo di crescita positivo di domanda e offerta, rafforzato dal programma di finanziamento Digital Europe.

In aggiunta, entro il 2030 l'UE effettuerà significativi avanzamenti riguardo all'onere per la sostenibilità e l'obiettivo di ottimizzare l'efficienza energetica e le performance dell'economia circolare del cloud computing e dei data center. Le aziende sviluppano, attivano e conseguono ambiziosi KPI di sostenibilità per mezzo di un utilizzo intelligente dei dati per gestire le supply chain da poco trasformate e l'innovazione tecnologica. Gli investimenti nelle soluzioni digitali green per affrontare le sfide del cambiamento climatico portano a ridotte emissioni di gas serra.

Il terzo ed ultimo scenario è quello definito *Challenge*, il quale mostra una spirale negativa che si auto-rinforza, al cui interno investimenti e domanda diminuiscono a causa di condizioni economiche globali meno favorevoli, portando così ad una crescita europea limitata. Si tratta di un mix di vari elementi, tra cui un contesto macroeconomico meno vantaggioso in confronto allo scenario baseline, condizioni di contesto meno convenienti e un'adozione più moderata dell'innovazione digitale, che porta ad un cammino di crescita limitata per il mercato dei dati. In questo scenario, sono presenti marcate disuguaglianze tra paesi economicamente avanzati (come ad esempio Stati Uniti, Francia e Germania) che investono in maniera continuativa su tecnologie digitali e innovazione dei dati e paesi con economie più fragili, meno capaci di restare aggiornati con le nuove tecnologie. In aggiunta, il suddetto contesto si distingue per flussi di dati frammentati e scarso livello di innovazione digitale ad opera delle PMI, con un singolo mercato digitale interno non completo e inadatto a supplire il divario tra i diversi paesi. Dal momento che la domanda sarà molto bassa, le dinamiche di domanda e offerta

saranno guidate dall'innovazione tecnologica. Pertanto, all'interno di questo scenario sono analizzati eventuali rischi e conseguenze legati all'incapacità di eliminare gli impedimenti al progresso dell'economia dei dati in Europa.

Nel sopraindicato contesto, è previsto un CAGR del PIL dell'UE tra 2025 e 2030 pari allo 0,8%, di molto minore rispetto all'1,6% dello scenario baseline. Questo rallentamento nella crescita economica si potrebbe additare a shock geopolitici come quello del conflitto tra Russia e Ucraina. Non solo, ci sarebbe la possibilità del manifestarsi di guerre commerciali scatenate da politiche protezionistiche oppure da un'altra crisi finanziaria, anticipata dall'incremento costante dell'inflazione e dei prezzi dell'energia. Nel caso in cui uno o più degli eventi sopraccitati si dovessero verificare, gli impatti sulla crescita dell'UE saranno determinati dalla robustezza dell'economia europea.

Una rilevante minaccia è quella di un elevato tasso di inflazione in quanto abbatte il potere d'acquisto delle persone dato che l'incremento dei salari reali non riesce a stare al passo con l'aumento dei prezzi. In questa ottica, tanto le misure sul lato dell'offerta quanto quelle sul lato della domanda andranno ad impattare in maniera ridotta e saranno attuate con maggiore lentezza. Inoltre, le misure di policy a sostegno dell'economia digitale risulteranno meno efficaci ed allo stesso tempo, gli investimenti pubblici in ricerca e sviluppo non saranno capaci di colmare adeguatamente la riduzione degli investimenti privati. A causa del carente sviluppo degli ecosistemi di dati in Europa, le piattaforme di condivisione dei dati sperimenteranno una limitata diffusione. L'assenza di standard comuni e livelli inadeguati di automazione rappresentano delle barriere che ostacolano la creazione di un unico mercato digitale equilibrato.

Dunque, sia il mercato che l'economia dei dati saranno nettamente minori in termini di valore economico nel 2030 in confronto allo scenario baseline. Più in dettaglio, le stime mostrano un valore del mercato pari all'incirca a 104 miliardi di euro con un CAGR dello 0,7%, mentre l'economia arriverà ad un valore di 723 miliardi di euro, equivalente al 5,2% del PIL dell'UE. Con un'innovazione digitale a rilento, l'economia legata alla spinta economica derivata da prodotti e servizi basati sui dati è ostacolata. Invece, per quanto riguarda le PMI, esse faticano a reggere il confronto con la concorrenza mondiale. I governi dispongono di risorse limitate per finanziare incentivi volti a promuovere la sostenibilità. Nel sopraccitato scenario, le imprese europee faticano a mantenere elevati livelli di investimenti digitali e preferiscono dedicare maggiori risorse alla sopravvivenza anziché accelerare la trasformazione digitale verso la sostenibilità. Inoltre, l'UE non riesce a raggiungere i suoi target di sostenibilità inerenti al green cloud. Non solo, il passaggio ad un'economia circolare e maggiormente efficiente sotto il profilo energetico procede ad un ritmo più lento e irregolare nell'intera Europa.

In conclusione, nonostante uno scenario internazionale articolato, caratterizzato da dinamiche contrastanti e segnato da continue tensioni geopolitiche, l'economia e il mercato dei dati dimostrano una straordinaria capacità di adattamento. Inoltre, anche se sono presenti pressioni interne e minacce esterne provenienti da paesi con modelli economici e valori politici differenti, l'Unione Europea continua a trarre vantaggio dalla crescita positiva della propria economia dei dati.

Conclusioni

Questo lavoro di tesi si pone come obiettivo quello di descrivere lo stato attuale e futuro dei machine data ed allo stesso tempo di mostrare il loro ruolo e gli impatti sui veicoli di nuova generazione.

Si parte con il mostrare i passi avanti fatti dalla tecnologia nel settore automotive e che sicuramente saranno al centro della mobilità del futuro, ripercorrendo le tappe storiche che hanno portato al loro sviluppo nel corso del tempo, per poi proseguire con un'analisi del mercato delle automobili connesse. Quest'ultimo risulta in continua crescita nei prossimi anni tanto a livello nazionale quanto a livello mondiale. Secondo le stime il mercato globale raddoppierà il suo valore economico in 6 anni passando da 12,4 a 26,4 miliardi di dollari. Per quanto riguarda quello italiano, nel 2023 ha raggiunto 1,56 miliardi di euro. In generale, i driver del mercato delle connected car sono sia le innovazioni tecnologiche che le novità normative come dichiarato da Giulio Salvadori, direttore dell'Osservatorio Connected Vehicle & Mobility del Politecnico di Milano.

Gli stakeholder coinvolti sono molti, ma per questione di praticità il lavoro si concentra su Carmaker, Assicurazioni, Gestori delle flotte e conducenti. Per tutti e quattro emergono numerosi benefici legati all'acquisizione di dati tramite i veicoli e riguardano vantaggi economici, maggiore sicurezza e ottimizzazione della gestione a 360 gradi dei mezzi di trasporto.

Successivamente il documento si focalizza sui dati. In primis, è presente un'analisi dettagliata per settori sul mercato europeo dei dati non personali che mostra l'incredibile varietà di compartimenti che trarrà importanti guadagni in termini economici. Nello specifico, i settori della finanza e delle attività estrattive e manifatturiere saranno i futuri protagonisti dei mercati dei dati non personali. Poi si passa ad un'analisi del mercato europeo complessivo dei dati, dalla quale si evince come i dati hanno contribuito in maniera sempre più significativa alla crescita e allo sviluppo dell'economia europea.

I Data Marketplace permettono di sfruttare i dati da un punto di vista economico e rappresentano una piattaforma che permette ai proprietari o detentori di dati di mettere in vendita i loro dati ed allo stesso tempo ai consumatori di comprare dati per una migliore profilazione dei loro clienti. Uno dei punti di forza è la varietà delle forme in cui si presentano.

Poter definire la valorizzazione, il valore e il prezzo dei dati non personali risulta complesso poiché tutti e tre dipendono da almeno due variabili, oltre ad essere influenzati dalla struttura del mercato. Riguardo a quest'ultima, quella che si avvicina maggiormente alla strategia europea dei dati è il mercato competitivo.

Dal punto di vista delle normative, il Data Act e il Data Governance Act rappresentano due strumenti fondamentali nelle mani della Commissione europea per poter realizzare spazi europei di condivisione dei dati. In particolare, l'intento delle suddette norme è quello di definire in maniera chiara la distribuzione di diritti ed obblighi per l'accesso e l'utilizzo dei dati ed incentivare la condivisione dei dati, migliorando la distribuzione dei benefici che si traggono da essi per poter diminuire il potere in mano alle big tech. Chiaramente solo il tempo potrà dire se entrambi i regolamenti riusciranno nel loro intento.

Trattando il tema dei dati, è emersa anche la questione della sicurezza informatica e della privacy che viene affrontata nel quarto capitolo. Tirando le somme, non risulta un quadro rasserenante per diversi motivi. Le cause automobilistiche non sembrano dare il giusto peso ai suddetti temi, in quanto hanno subito e continuano a subire vari attacchi cibernetici. Anche per quanto riguarda la privacy ci sono delle criticità come emerso dallo studio della Mozilla Foundation e da quello condotto da Privacy4Cars. Inoltre, dalla ricerca effettuata dalla Federazione Internazionale dell'Automobile si evince come gli stessi consumatori siano confusi e ignoranti rispetto al veicolo che guidano e ai dati che raccoglie. Allo stesso tempo però si può apprezzare la presenza di iniziative positive come quella dello strumento Vehicle Privacy Report e del Global Automotive Security Test Center che hanno come obiettivo la tutela della privacy e della sicurezza dei guidatori. Data la rilevanza della questione, anche le organizzazioni governative si sono attivate, definendo due nuove norme (R155 e R156 dello United Nations Economic Commission for Europe) che hanno come obiettivo quello di imporre che la sicurezza informatica dei veicoli sia una condizione essenziale da rispettare lungo tutto il ciclo di vita di un veicolo e che riguarda ogni attore presente lungo l'intera supply chain e non solo la casa automobilistica.

Successivamente si illustra uno dei temi più discussi nel settore automotive, ovvero la guida autonoma. Dagli studi della McKinsey and Company si può concludere che sicuramente gli ADAS e la guida autonoma saranno sempre più protagonisti all'interno dei veicoli, anche se la rapidità con cui ciò avverrà dipende dall'evolversi del settore automotive. Inoltre, porteranno alla generazione di importanti flussi economici. Non solo, gli stessi guidatori dimostrano un forte interesse tanto per gli ADAS quanto per la guida autonoma, tuttavia c'è ancora molto lavoro da fare affinché le persone si sentano veramente a proprio agio nel viaggiare su di una vettura senza conducente.

Per concludere, la tesi offre uno sguardo a quello che potrebbe essere il futuro del mercato e dell'economia dei dati all'interno dell'Europa, tenendo in considerazione i conflitti bellici attuali e quelli potenziali, oltre alla politica estera del nuovo presidente degli Stati Uniti. Al di là di come si evolveranno le varie questioni geopolitiche, secondo le stime, tanto il mercato quanto l'economia dei dati cresceranno positivamente contribuendo in maniera notevole al PIL dell'Europa.

Bibliografia e sitografia

<https://www.europarl.europa.eu/news/it/press-room/20230310IPR77226/data-act-nuove-regole-per-un-accesso-e-utilizzo-dei-dati-piu-equivo#:~:text=80%25%20dei%20dati%20non%20utilizzati,centro%20delle%20relazioni%20tra%20imprese.>

<https://www.lexibc.com/en/eu-data-act-2023-what-it-establishes/>

<https://digital-strategy.ec.europa.eu/it/policies/strategy-data>

<https://innowise.com/it/blog/big-data-trends-2024/>

https://ec.europa.eu/commission/presscorner/detail/it/ip_22_1113

<https://themarkup.org/the-breakdown/2022/07/27/who-is-collecting-data-from-your-car>

<https://www.wallstreetitalia.com/auto-a-guida-autonoma-cresce-il-mercato-nonostante-gli-incidenti/>

<https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/autonomous-drivings-future-convenient-and-connected>

<https://www.agendadigitale.eu/mercati-digitali/automobili-connesse-la-sfida-della-privacy-obiettivi-e-ostacoli/>

<https://www.economyup.it/automotive/connected-car/>

<https://www.autopi.io/glossary/vehicle-to-everything/>

<https://blog.rgbsi.com/7-types-of-vehicle-connectivity>

Malik, Rami & Ramli, Khairun & Kareem, Zahraa & Habelalmate, Mohammed & Abbas, Ali & Alamoody, Abdulla. (2020). *An Overview on V2P Communication System: Architecture and Application*. 174-178. 10.1109/IICETA50496.2020.9318863.

<https://www.flexihub.com/vehicle-to-network/>

[https://www.compassiot.com.au/media/the-different-types-of-vehicle-connectivity#:~:text=Vehicle%20to%20Cloud%20\(V2C\),drivers'%20seat%20and%20mirror%20preferences](https://www.compassiot.com.au/media/the-different-types-of-vehicle-connectivity#:~:text=Vehicle%20to%20Cloud%20(V2C),drivers'%20seat%20and%20mirror%20preferences)

Umar Zakir Abdul Hamid, and publisher SAE International. *Autonomous, Connected, Electric and Shared Vehicles : Disrupting the Automotive and Mobility Sectors*. 1st ed. Warrendale, Pennsylvania: SAE International, 2022. Print.

<https://teoriadeisegnali.it/blog/items/vehicular-ad-hoc-networks/>

https://blog.osservatori.net/cos-e-smart-car-come-funziona?_gl=1*vfdkc8*_ga*NjYyMjExODU1LjE3MjkwNjY3MzQ.*_ga_8JFFBZLKC3*MTczMDExOTU3My44LjEuMTczMDExOTU3My4wLjAuMA..

<https://blog.rgbsi.com/what-is-v2i-technology>

Lu, Sidi, and Weisong Shi. *Vehicle Computing : From Traditional Transportation to Computing on Wheels*. 1st ed. 2024. Cham: Springer Nature Switzerland, 2024. Web.

<https://www.bmw.com/it/innovation/connected-car.html>

<https://www.fueloyal.com/what-is-connected-vehicle-and-history-of-connected-vehicles/>

<https://www.autoconnectedcar.com/auto-connected-car-news-connected-car-history-and-timeline/>

<https://www.cargurus.co.uk/Cars/articles/what-is-mirrorlink>

<https://ei.futuranet.it/2024/06/17/perche-gli-aggiornamenti-ota-sono-importanti-nelliot/>

<https://www.eunews.it/2015/04/28/sara-obbligatorio-sulle-auto-lallarme-automatico-caso-di-incidenti-e-call/>

<https://www.hivepower.tech/it//blog/tutto-quello-che-devi-sapere-su-v1g-v2h-v2b-v2g-e-v2x>

<https://www.embitel.com/blog/embedded-blog/no-android-auto-is-not-an-infotainment-os-make-way-for-android-automotive>

<https://www.ilsole24ore.com/art/auto-e-camion-2022-sistemi-sicurezza-elettronici-obbligatorii-tutti-veicoli-ACJKGix>

<https://www.autoconnectedcar.com/2016/08/connected-cars-know-when-lights-turn-green-soon/>

<https://www.press.bmwgroup.com/italy/article/detail/T0280987IT/20-anni-all%E2%80%99avanguardia:-bmw-connecteddrive?language=it>

<https://www.marketsandmarkets.com/Market-Reports/connected-car-market-102580117.html>

<https://www.economyup.it/automotive/connected-car-mobility-sempre-piu-auto-connesse-soluzioni-sostenibili-e-smart-road/>

<https://www.economyup.it/automotive/connected-car-in-crescita-nel-mondo-in-italia-una-ogni-4-abitanti/>

https://www.repubblica.it/green-and-blue/dossier/viaggio-al-centro-del-futuro-ok/2024/08/22/news/auto_connesse_mercato_in_crescita_la_spinta_della_telematica_e_della_guida_autonoma-423457818/

<https://etsc.eu/about-us/>

<https://www.omrglobal.com/industry-reports/connected-car-market>

<https://www.eetimes.eu/how-can-oems-use-connected-vehicle-sensor-data/>

https://blog.osservatori.net/it_it/ecall-obbligatorio-auto-connessa

<https://www.ilsole24ore.com/art/ecall-chiamata-d-emergenza-diventa-obbligatoria--AEq5RTQE>

https://europa.eu/youreurope/citizens/travel/security-and-emergencies/emergency-assistance-vehicles-ecall/index_it.htm

<https://www.expressvpn.com/it/blog/how-your-smart-car-tracks-you/>

<https://themarkup.org/the-breakdown/2022/07/27/who-is-collecting-data-from-your-car>

<https://www.autopi.io/glossary/car-sensors-types-functions/>

<https://www.exav.it/blog/side-automotive-sistemi-adas-obblighi-2024-per-una-guida-piu-sicura-e-smart/>

https://www.alvolante.it/da_sapere/tecnica/adas-cosa-sono-e-quali-sono-piu-importanti-380565

https://www.alvolante.it/da_sapere/sicurezza/nuovi-adas-obbligatori-auto-luglio-2024-382514

https://www.quattroruote.it/news/sicurezza/2024/01/31/sicurezza_stradale_ecco_come_funziona_la_black_box_incorporata_nelle_auto.html

<https://www.arrow.com/it-it/research-and-events/articles/sensor-technologies-in-the-modern-vehicle>

<https://www.quattroruote.it/guide/componenti-auto/head-up-display.html>

[Regolamento \(CE\) 2019/2144 relativo ai requisiti di omologazione dei veicoli a motore e dei loro rimorchi, nonché di sistemi, componenti ed entità tecniche destinati a tali veicoli, per quanto riguarda la loro sicurezza generale e la protezione degli occupanti dei veicoli e degli altri utenti vulnerabili della strada](#)

<https://www.moneygeek.com/insurance/auto/telematics-definition/>

<https://www.generali.it/magazine/auto/scatola-nera>

<https://www.insurethebox.com/telematics>

<https://www.assicurazione.it/guide/scatola-nera-assicurazione-auto-cos-e-come-funziona.html>

<https://ims.tech/knowledge-hub/what-is-mobile-app-telematics/>

<https://ims.tech/knowledge-hub/mobile-telematics-apps-auto-insurance/>

Hong-Jie Li, Xing-Gang Luo, Zhong-Liang Zhang, Wei Jiang, Shen-Wei Huang, *Driving risk prevention in usage-based insurance services based on interpretable machine learning and telematics data*, Decision Support Systems, Volume 172, 2023, 113985, ISSN 0167-9236, (<https://www.sciencedirect.com/science/article/pii/S016792362300060X>)

L. Cunha and J. M. Bravo, "Automobile Usage-Based-Insurance: Improving Risk Management using Telematics Data," 2022 17th Iberian Conference on Information Systems and Technologies (CISTI), Madrid, Spain, 2022, pp. 1-6, doi: 10.23919/CISTI54924.2022.9820146.

<https://www.lumi4innovation.it/iot-gestione-flotte/>

<https://www.atatus.com/glossary/machine-data/>

Calzolari, Giacomo and Cheysson, Anatole and Rovatti, Riccardo, *Machine Data: Market and Analytics* (January 23, 2023). Available at SSRN: <https://ssrn.com/abstract=4335116>

Batura, O., Wion, A., Gonzalez, S. N., Marcus, J. S., Godlovitch, I., Wiewiorra, L., Kroon, P., Tas, S., and Steffen, N., 2023, *The Emergence of non-personal data markets*, Publication for the committee on Industry, Research and Energy (ITRE), Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg.

<https://digital-strategy.ec.europa.eu/library/results-european-data-market-study-2021-2023>

M. Zhang, F. Beltrán and J. Liu, "A Survey of Data Pricing for Data Marketplaces," in IEEE Transactions on Big Data, vol. 9, no. 4, pp. 1038-1056, 1 Aug. 2023, doi: 10.1109/TBDDATA.2023.3254152.

<https://datarade.ai/company/blog/data-marketplaces>

<https://research.aimultiple.com/data-marketplace/#what-is-a-data-marketplace>

Galiano, A. et al. 2020. I dati non personali: la natura e il valore. *Rivista italiana di informatica e diritto*. 2, 1 (Mar. 2020), 61–77

<https://digital-strategy.ec.europa.eu/it/policies/strategy-data>

Crepax T, Gaur M and da Rosa Lazarotto B. *Measuring data access and re-use in the European Legal Framework for Data, from the General Data Protection Regulation (GDPR) law to the Proposed Data Act: the case of vehicle data* [version 1; peer review: 1 approved, 3 approved with reservations]. Open Res Europe 2023, 3:192 (<https://doi.org/10.12688/openreseurope.16468.1>)

Groza, Teodora and Botero Arcila, Beatriz. "The New Law of the European Data Markets: Demystifying the European Data Strategy" *Global Jurist*, vol. 24, no. 3, 2024, pp. 321-364. <https://doi.org/10.1515/gj-2024-0045>

Regolamento generale sulla protezione dei dati (GDPR - https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ITA&toc=OJ:L:2016:119:TOC)

Data Governance Act (<http://data.europa.eu/eli/reg/2022/868/oj>)

Data Act (<http://data.europa.eu/eli/reg/2023/2854/oj>)

Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo (normativa sui dati - <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52022PC0068>)

Poletti D, 'Gli intermediari dei dati' (2022) 1 EJPLT, 45-56. DOI: <https://doi.org/10.57230/EJPLT221DP>

S. Jayakumar, A. S. Sadiq, S. Hamdare and O. Kaiwartya, "Driving Safely in the Digital Age: Securing Connected Cars Against Cyber Threats," 2024 IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS), Shah Alam, Malaysia, 2024, pp. 151-156, doi: 10.1109/I2CACIS61270.2024.10649859.

<https://www.alvolante.it/news/maxi-data-breach-clienti-toyota-384219>

<https://www.latimes.com/business/autos/la-fi-hy-musk-computer-on-wheels-20150319-story.html>

<https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/>

<https://www.agendadigitale.eu/mercati-digitali/automobili-connesse-la-sfida-della-privacy-obiettivi-e-ostacoli/>

<https://startupitalia.eu/tech/cybersecurity/cose-e-cosa-fara-il-nuovo-global-automotive-security-test-center-di-ntt-data-in-italia/>

<https://it.motor1.com/news/622433/ntt-data-centro-test-cybersecurity/>

https://www.repubblica.it/motori/sezioni/tecnologia-e-ambiente/2022/06/30/news/allarme_cybersicurezza_ecco_le_nuove_regole_per_proteggere_lauto-356009646/

<https://www.nexta.bureauveritas.it/newsroom/cybersecurity-nel-settore-automotive-la-regulation-155-impone-la-security-design#:~:text=La%20Unece%20R155%20entrer%C3%A0%20in,ottenere%20l'omologazione%20del%20veicolo.>

<https://www.dqsglobal.com/it-it/imparare/blog/sicurezza-informatica-nel-settore-automobilistico-nuovi-regolamenti-obbligatorii#automotive-cyber-security-neue-verbindliche-vorschriften-chapter07>

<https://autocrypt.io/unr156-securing-vehicle-software-updates/>

<https://www.techeconomy2030.it/2015/07/22/connectedcar-hacker-prendono-controllo-jeep-cherokee-in-autostrada/>

<https://web.aci.it/comunicazione/auto-connesse-allarme-fia-sui-dati/>

A. A. Riffée, A. Riffée and T. A. Youssef, "Connected Vehicle Security: Overview of Risks and Mitigation Strategies," SoutheastCon 2024, Atlanta, GA, USA, 2024, pp. 1432-1437, doi: 10.1109/SoutheastCon52093.2024.10500211.

[https://ecudigital.it/come-funziona-una-centralina-elettronica-ecu-dell'auto/#:~:text=Cos'%C3%A8%20una%20Centralina%20Elettronica%20\(ECU\)%3F&text=La%20sua%20principale%20funzione%20%C3%A8,del%20carburante%20e%20molto%20altro](https://ecudigital.it/come-funziona-una-centralina-elettronica-ecu-dell'auto/#:~:text=Cos'%C3%A8%20una%20Centralina%20Elettronica%20(ECU)%3F&text=La%20sua%20principale%20funzione%20%C3%A8,del%20carburante%20e%20molto%20altro)

<https://www.cybersecurity360.it/news/hyundai-sotto-attacco-violati-dati-di-clienti-italiani-e-francesi-cosa-sappiamo/>

<https://www.bleepingcomputer.com/news/security/hyundai-motor-europe-hit-by-black-basta-ransomware-attack/>

P. Grümer and P. Brandão, "An Automotive Cybersecurity Maturity Level Assessment Programme," 2023 53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W), Porto, Portugal, 2023, pp. 84-91, doi: 10.1109/DSN-W58399.2023.00035.

Vellinga, N. E. (2022). Connected and vulnerable: cybersecurity in vehicles. *International Review of Law, Computers & Technology*, 36(2), 161–180. <https://doi.org/10.1080/13600869.2022.2060472>
<https://www.alvolante.it/news/brevetto-ford-non-paghi-rate-auto-sequestra-da-sola-383097>

<https://www.athlon.com/it/blog/veicoli-autonomi-e-intelligenza-artificiale-il-futuro-della-guida-automobilistica/>

https://www.alvolante.it/da_sapere/tecnologia/5-livelli-della-guida-autonoma-396147

S. Atakishiyev, M. Salameh, H. Yao and R. Goebel, "Explainable Artificial Intelligence for Autonomous Driving: A Comprehensive Overview and Field Guide for Future Research Directions," in IEEE Access, vol. 12, pp. 101603-101625, 2024, doi: 10.1109/ACCESS.2024.3431437.

Simon Burton, Ibrahim Habli, Tom Lawton, John McDermid, Phillip Morgan, Zoe Porter, *Mind the gaps: Assuring the safety of autonomous systems from an engineering, ethical, and legal perspective*, Artificial Intelligence, Volume 279, 2020, 03201, ISSN 0004-3702, <https://doi.org/10.1016/j.artint.2019.103201>.
(<https://www.sciencedirect.com/science/article/pii/S0004370219301109>)

<https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/autonomous-drivings-future-convenient-and-connected>

<https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/hands-off-consumer-perceptions-of-advanced-driver-assistance-systems>

<https://www.mimit.gov.it/it/incentivi/fondo-ipcei-importanti-progetti-di-comune-interesse-europeo>

<https://it.tradingview.com/news/invezz:a960b74d46c55:0/>

Ringraziamenti

Eccomi finalmente giunto alla conclusione di questo percorso di studi. Non è stato semplice, anzi tutt'altro, però proprio per questo mi ha permesso di crescere sia da un punto di vista professionale che personale. Sono diverse le persone che hanno contribuito al raggiungimento del mio traguardo e che ringrazio per essere state sempre presenti in questa lunga avventura.

Il professore Carlo Cambini, che con i suoi suggerimenti ha consentito la realizzazione di questa tesi.

La mia famiglia che mi ha supportato ed è stata al mio fianco durante tutto questo tempo, fornendomi preziosi consigli, spronandomi e che mi ha insegnato a non mollare davanti a nessun ostacolo e a proseguire diritto verso l'obiettivo.

Gli amici, quelli che ormai conosco da ben 12 anni e altri da molto meno, con i quali ho condiviso avventure e momenti indimenticabili.

Grazie di cuore a tutti voi.