UNIVERSITA' DEGLI STUDI DI ROMA TOR VERGATA

***European Digital Law of the Person, of the Contract and of the Technological Marketplace* - EUDILA**
Cattedra Jean Monnet del Progetto ERASMUS +

SMART CARS E DATA PROTECTION:

Il trattamento dei dati personali

Francesca Filippucci

0348910

Anno accademico 2023/2024

Indice

Abstract

L'Internet of Things (IoT) costituisce l'attuale era digitale in cui gli oggetti della vita quotidiana sono sempre più interconnessi tramite Internet: si stima che il numero di tali dispositivi supererà i trenta miliardi entro il 2025, ovvero una media di quattro dispositivi per persona. Le tecnologie IoT stanno trovando larga applicazione nel settore automotive: in Italia il mercato delle Smart Cars costituisce la principale aerea di investimento dell' IoT, rappresentando il 18% del totale con un fatturato di 1,5 miliardi di euro.[1] I veicoli, dunque, finiscono per diventare dei veri e propri data hub in cui strumenti tecnologici e sensori captano informazioni tecniche ma anche riguardanti la geolocalizzazione, le abitudini di vita e i dati biometrici relativi a conducenti e passeggeri. La raccolta e la trasmissione di queste tipologie di dati apre questioni giuridiche rilevanti nell'ambito della data protection: la profilazione degli utenti, la possibilità di utilizzo improprio dei dati e la violazione dei sistemi informatici. Il presente trattato si propone di analizzare le criticità legate al trattamento dei dati personali raccolti dai veicoli connessi, con particolare riferimento al Regolamento Generale sulla Protezione dei Dati (GDPR)[2] e alle Linee Guida 01/2022[3] rilasciate dall'European Data Protection Board (EDPB). Si valuterà la liceità del trattamento, con attenzione alla qualità del consenso rilasciato da parte degli utilizzatori del veicolo connesso, fornendo inoltre una panoramica sulle misure di tutela della privacy che si possono mettere in atto per mitigare tali rischi. Infine, verrà presentato un esempio di trattamento di dati personali nell'ambito delle Smart Cars, ovvero le assicurazioni "Pay as you drive".

[1] Smart building e Smart City, a che punto siamo: il mercato IoT in Italia, Proptech 360. https://www.proptech360.it/mercato/smart-building/smart-building-e-smart-city-a-che-punto-siamo-il-mercato-iot-in-italia/

[2] Regolamento Eu 679/2016.

[3] EDPB, Linee guida 01/2020 sul trattamento dei dati personali nel contesto dei veicoli connessi e delle applicazioni legate alla mobilità, Versione 2.0, 9/3/2021.

1.Smart Cars e raccolta dei dati personali

1.1.Le Smart Cars e i sistemi ADAS

Per Smart Car si intende un'auto intelligente in grado di connettersi ad internet per scambiare informazioni con altri veicoli, con l'infrastruttura e l'ambiente circostante. La diffusione delle Smart Cars annovera tra i potenziali benefici la riduzione della congestione del traffico e dei livelli di consumo, ma anche un miglioramento della sicurezza stradale e del tasso di inquinamento. Un settore ancora in fase sperimentale è quello dei veicoli a guida autonoma, che permetterebbero di offrire una mobilità più accessibile per tutti. Attualmente la tecnologia più comune sui veicoli è quella della "scatola nera" (ovvero box GPS/GPRS), che localizza il veicolo e tiene traccia delle informazioni utili per ricostruire le dinamiche di incidente. Ciò che, però, giustifica la crescita nel mercato delle autovetture smart sono i veicoli nativamente connessi.[4] Infatti, a partire dal Luglio 2022, il Regolamento sulla sicurezza dei veicoli[5] prevede che le auto di nuova omologazione siano dotate di dispositivi elettronici e di assistenza alla guida, basati sull'utilizzo di sensori, radar, videocamere e computer di bordo, al fine di ridurre il rischio di sinistri. Tra questi, oltre alla già citata scatola nera integrata nel veicolo dalla casa madre, si evidenziano i sistemi di assistenza alla vita ADAS (Advanced Driver Assistance System) divenuti obbligatori[6]:

- Intelligent Speed Assistance (ISA): sistema in grado di intervenire sulla velocità del veicolo al fine del rispetto dei limiti di velocità;
- Emergency Lane Keeping Assist (ELKA): in caso di superamento della linea continua della carreggiata, questo sistema riporta il veicolo verso il centro della corsia;
- Autonomous Emergency Braking (AEB): sistema autonomo di frenata in caso di emergenza;
- Driver Monitor System (DMS): sistema che, riprendendo i movimenti oculari attraverso l'uso di telecamere interne, è in grado di rilevare il livello di attenzione del guidatore anticipando i segnali di sonnolenza;
- Alcolock o Ignition Interlock Device (IID): etilometro da auto che alla registrazione di un tasso alcolemico sopra la norma non permette l'accensione del motore.

[4]Smart Car, auto intelligenti e connesse a guida del futuro, Osservatorio del Politecnico di Milano. https://blog.osservatori.net/it_it/smart-car-auto-intelligenti-connesse
[5] Regolamento Eu 2019/2144
[6] https://www.alvolante.it/da_sapere/tecnica/adas-cosa-sono-e-quali-sono-piu-importanti-380565

Altri sistemi ADAS comuni sono il sistema di rilevamento dei pedoni, sensori di parcheggio, ma anche di monitoraggio dello stato di salute del veicolo (informazione sulla pressione dei penumatici, sul buon funzionamento del motore, etc). La Pratica raccomandata SAE J3016[7] distingue sei diversi livelli di automazione della guida per i veicoli a motore, che vanno dal Livello 0 (nessuna automazione alla guida) al Livello 6 (totale automazione nella guida). L'evoluzione dei sistemi ADAS è orientata verso l'automazione completa con sistemi di sicurezza preveggenti e sempre più connessi con le altre vetture, ad oggi si stanno perfezionando i risultati legati al livello 4 (Guida autonoma alta) e livello 5.[8]

1.2.I dati generati dalle Smart Cars

Il Comitato Europeo per la Protezione dei Dati (EDPB) nelle Linee Guida 01/2020[9] caratterizza il veicolo connesso come un insieme di centraline elettroniche di controllo (ECU) , collegate attraverso una rete di bordo e dotate di sistemi di connettività funzionali per lo scambio di informazioni con altri dispositivi, sia all'interno che all'esterno dei veicoli. Si individuano, inoltre, come ambito di applicazione tre diverse tipologie di dati: quelli raccolti ed elaborati all'interno del veicolo, quelli trasmessi dal veicolo a dispositivi mobili ad essi collegati (ad esempio le app autonome sul telefono dell'utente) e quelli raccolti nel veicolo ma trasmessi ad entità esterne (case costruttrici, gestori di infrastrutture, assicurazioni). Tra questi vi sono sia dati relativi al funzionamento del veicolo sia informazioni che, direttamente o indirettamente, possono consentire un'identificazione delle persone fisiche: basti pensare ai dettagli circa lo spostamento di un soggetto che potrebbero rivelare informazioni sullo stile di vita, sul luogo di lavoro o riguardo l'orientamento politico e religioso (a seconda, ad esempio, dei luoghi frequentati). Dal momento che ogni veicolo è registrato tramite il numero di identificazione (VIN), anche i dati tecnici potrebbero rimandare ad una persona fisica, oltre che divenire informazioni rilevanti, ad esempio, per compagnie assicurative o produttori di automobili (si pensi allo stile di guida del conducente o lo stato di usura del veicolo). Per queste ragioni i garanti Europei riconoscono che i dati trattati dalle Smart Cars costituiscono dati personali ai sensi dell'articolo 4 del GDPR. E' infatti definito dato personale "qualsiasi informazione riguardante una persona fisica identificata o identificabile", ovvero che vi si possa risalire

[7] Tassonomia e definizioni relativi ai sistemi di automazione della guida per veicoli a motore su strada, Society of Automotive Engineering, SAE J3016

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

[9] EDPB, Linee guida 01/2020 sul trattamento dei dati personali nel contesto dei veicoli connessi e delle applicazioni legate alla mobilità, Versione 2.0, adottate il 9/3/2021.

direttamente o indirettamente, "con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale".[10] Inoltre va sottolineato che parte dei dati generati dai veicoli connessi potrebbero rientrare nella definizione di dati "sensibili" e dunque meritare ulteriore attenzione: nell'Art.9 del GDPR vengono definiti come tali tutti i dati che "rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi ad indentificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona".[11] Le linee guida 01/2020 individuano, in particolare, tre tipologie di dati trattati nelle Smart Cars che rientrano nella classificazione di dati sensibili e dunque hanno un maggiore impatto sui diritti dei soggetti interessati:

- Dati relativi all'ubicazione: rilevanti perché permettono di risalire alle abitudini di vita del conducente;
- Dati biometrici: utilizzati per l'accesso al veicolo, l'autentificazione del conducente e l'accesso alle impostazioni del suo profilo che permettono l'identificazione univoca della persona fisica;
- Dati che rivelano reati o altre violazioni: la combinazione di alcune categorie di dati raccolti dai veicoli connessi, ad esempio l'informazione del superamento di una linea della carreggiata con quella della posizione geografica e della velocità istantanea del veicolo, potrebbero rivelare la commissione di una violazione. Nel caso in cui questi dati venissero utilizzati a fini di indagine entrerebbero in campo i requisiti previsti dall'Art.10 del GDPR.

1.3.Rischi e privacy

Inoltre con l'aumentare delle funzionalità messe a disposizione dai veicoli connessi tenderanno a crescere anche le quantità di dati raccolti, che potrebbero risultare eccedenti rispetto a quelli realmente necessari per lo scopo. In particolare, l'applicazione di algoritmi machine learning prevede un apprendimento automatico a partire da una larga base di dati a disposizione, mantenuti per un lasso temporale prolungato. Parallelamente si incrementeranno anche i servizi offerti e le

[10] Art4,GDPR.
[11] Art9,GDPR.

modalità di connessione (USB,WI-FI,WEB), che potrebbero esporre le smart cars ad una maggiore vulnerabilità riguardo potenziali attacchi e alla compromissione dei dati. I dati personali archiviati nel veicolo o esternamente ad esso, vedi il cloud computing, dovrebbero essere tutelati da accessi non autorizzati: nelle sopracitate Linee Guida si fa l'esempio di un meccanico che deve poter accedere solamente ai dati tecnici necessari per un'eventuale riparazione e non a tutti i dati memorizzati nel dispositivo. Il Gruppo di lavoro Articolo 29[12] per la protezione dei dati già nel 2014 aveva espresso preoccupazione sulle criticità legate alla sicurezza e al controllo dei dati nell'ambito dell'Internet of Things: con riferimento alle Smart Car queste preoccupazione acquisiscono ulteriore rilievo, dato che una violazione del sistema potrebbe mettere a rischio la sicurezza degli utilizzatori e di chi li circonda. In tale senso è emblematico il caso di un gruppo di hacker che nel 2016 sono riusciti a prendere il controllo di una Tesla Model S[13] interferendo con il corretto funzionamento di freni, serrature delle portiere e schermo del cruscotto da 12 miglia di distanza. In un'ottica di progressivo avanzamento verso la guida autonoma, la sicurezza informatica e la protezione dei dati sono un tema centrale. Alla luce di quanto detto, risulta rilevante l'aspetto del diritto alla privacy degli utenti, che rischia di essere compromesso dal largo sfruttamento di dati che avviene all'interno delle Smart Cars. Tale diritto subisce un'evoluzione nella sua definizione, anche per effetto dello sviluppo tecnologico. Si passa da una concezione negativa della riservatezza ,come "diritto ad essere lasciato solo",[14] ad una visione più positiva come diritto alla protezione dei dati. Secondo questa nuova ottica i dati circolano anche nell'interesse degli utenti coinvolti, che devono però poter esercitare un controllo attivo sui propri dati. Nonostante il Diritto alla privacy non sia definito come diritto fondamentale, l'Art.2 della Costituzione lo tutela indirettamente dal momento che è stato ben presto interpretato come una clausola aperta atta a ricomprendere tutti i diritti che rappresentano l'essere stesso della persona. Un primo riconoscimento di tale diritto viene effettuato con la Legge n. 675 del 1996[15], a seguire un' ulteriore menzione vi è nella Carta dei diritti fondamentali dell'Unione Europea dove nell'Art. 7 si legge: "Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni". La legislazione in tema di Privacy viene raccolta, inoltre, nel Decreto Legislativo 196 del 30 Giugno del 2003, noto come Codice della Privacy, poi modificato nel 2018 con l'entrata in vigore del Regolamento Generale

[12] Gruppo di Lavoro Articolo 29- Parere 8/2014 sui recenti sviluppi nel campo dell'Internet degli oggetti https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_it.pdf
[13] Team of Hacker take remote control of Tesla Model S from 12 miles away, The Guardian, 2016
[14] Ubertazzi, Il diritto alla Privacy, Natura e funzioni giuridiche, 2004
[15] Legge sulla Protezione dei Dati Personali, Legge n. 675, 1996

sulla Protezione dei Dati (GDPR), regolamento 679 del 2016. Il GDPR costituisce il regolamento Europeo Privacy intitolato alla tutela delle persone fisiche, con riguardo al trattamento dei dati e alla libera circolazione dei dati. Questo concretizza una presa d'atto dell'incremento dello sviluppo tecnologico e delle sue potenzialità: l'impostazione del regolamento privacy è orientata alla tutela del diritto fondamentale della persona, ma comunque coniugata con la volontà di incentivare la circolazione dei dati per la creazione di un mercato europeo unico dei dati.

1.4.Base giuridica di riferimento

Avendo appurato che i dati trattati dal veicolo connesso sono dati personali, il quadro giuridico Europeo di riferimento è da individuare principalmente nel GDPR. In aggiunta a questo, si deve considerare la Direttiva 2002/58/CE[16] relativa alla vita privata e alla comunicazioni elettroniche, poi modificata dalla direttiva 2009/136/CE[17] (anche nota come direttiva e-Privacy). Tale direttiva esprime indicazioni principalmente rivolte a fornitori di servizi di comunicazione elettronica accessibili al pubblico e a fornitori di reti pubbliche di comunicazione, eppure nell'Art.5 paragrafo 3 si trova una trattazione di carattere generale: si fa riferimento a "qualsiasi soggetto, sia esso pubblico o privato, che registri o legga informazioni su un'apparecchiatura terminale indipendentemente dalla natura dei dati che sono archiviati o a cui si accede"[18]. Tale articolo trova applicazione, dunque, nella presente area di indagine dal momento che il veicolo connesso ed i dispositivi a esso associati posso rientrare nella definizione di "apparecchiature terminali". Questa espressione viene definita dalla direttiva 2008/63/CE[19] all'Art. 1: "a) le apparecchiature allacciate direttamente o indirettamente all'interfaccia di una rete pubblica di telecomunicazioni per trasmettere, trattare o ricevere informazioni; in entrambi i casi di allacciamento, diretto o indiretto, esso può essere realizzato via cavo, fibra ottica o via elettromagnetica; un allacciamento è indiretto

[16] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, Gazzetta Ufficiale n. L 201 del 31/07/2002

[17] Direttiva 2009/136/CE del Parlamento Europeo e del Consiglio, 25 novembre 2009 recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori https://www.edps.europa.eu/sites/default/files/publication/dir_2009_136_it.pdf

[18] EDPB, Linee guida 01/2020 sul trattamento dei dati personali nel contesto dei veicoli connessi e delle applicazioni legate alla mobilità, Versione 2.0, adottate il 9/3/2021.

[19] Direttiva 2008/63/CE della Commissione del 20 Giugno 2008 relativa alla concorrenza sui mercati delle apparecchiature terminali di telecomunicazioni https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32008L0063&from=GA

se l'apparecchiatura è interposta fra il terminale e l'interfaccia della rete pubblica; b) le apparecchiature delle stazioni terrestri per i collegamenti via satellite". Riguardo l'interazione tra la direttiva e-privacy e il GDPR si è espresso l'EDPB con il parere 5/2019[20]: l'articolo 5 della direttiva e-Privacy prevede che per effettuare l'archiviazione di informazioni o l'accesso ad informazioni già archiviate nelle apparecchiature terminali di un utente sia necessario il suo consenso. Il Garante europeo sancisce che l'articolo 5 sopracitato prevalga sull'articolo 6 del GDPR, relativamente alle attività di archiviazione o di accesso alle informazioni contenute nel dispositivo che costituiscano dati personali mentre, per quanto riguarda le operazioni di trattamento successive a quelle menzionate (tra cui il trattamento di dati personali ottenuti dall'accesso all'apparecchiatura terminale), devono avere fondamento giuridico secondo l'Art.6 del GDPR, che ne definisce la liceità. Dunque " i titolari del trattamento non possono invocare l'articolo 6 del GDPR per ridurre l'ulteriore tutela offerta dall'articolo 5, paragrafo 3, della direttiva e-privacy".[21] L'obbligo di consenso previsto dalla direttiva si sospende nei casi in cui l'operazione abbia il solo scopo di trasferire un' informazione su una rete di comunicazione elettronica o sia necessaria per permettere di erogare un servizio esplicitamente richiesto dall'utente o abbonato.

[20] Comitato Europeo per la protezione dei dati, Parere 5/2019 sull'interazione tra la direttiva e privacy e il regolamento generale sulla protezione dei dati, in particolare per quanto concerne competenze, compiti e poteri delle autorit per la protezione dei dati, adottato il 12 marzo 2019,punto 40 e 41.

[21] EDPB, Linee guida 01/2020 sul trattamento dei dati personali nel contesto dei veicoli connessi e delle applicazioni legate alla mobilità, Versione 2.0, adottate il 9/3/2021

2.Il trattamento dei dati personali nelle Smart Cars

I dati raccolti dai veicoli connessi vengono gestiti in un ambiente molto articolato, che non coinvolge solo le classiche aziende automobilistiche, ma attira anche nuovi protagonisti del mercato digitale: vi sono aziende interessate ad offrire servizi di intrattenimento (musica on-line, informazioni sulla viabilità), sistemi di assistenza alla guida (software di guida autonoma, aggiornamenti sulle condizioni di veicolo, assicurazioni basate sull'uso). Inoltre, data la necessità dei veicoli smart di essere costantemente connessi, entrano in gioco anche i gestori delle infrastrutture stradali e gli operatori di telecomunicazione come possibili esecutori di un trattamento di dati propri degli utilizzatori del veicolo. L'Art.4 del GDPR, al punto 2, definisce il trattamento come qualsiasi operazione riguardante dati personali, con o senza l'ausilio di processi automatizzati, che comprenda la raccolta, la registrazione, l'organizzazione, la modifica, la consultazione, l'utilizzo, la condivisione, la cancellazione, ecc.

2.1.Soggetti e princìpi del trattamento

Di seguito, verranno illustrate i principali soggetti coinvolti nel trattamento, con riferimento all'ambito di trattazione preso in esame.

- **L'interessato**: la persona fisica a cui appartengono i dati trattati[22]. Con riferimento ai veicoli connessi, può essere il conducente (occasionale o non), il passeggero o il proprietario del veicolo.
- **Il titolare del trattamento**: l'entità che "determina le finalità e i mezzi del trattamento di dati personali".[23] Può essere un fornitore di servizi che, ad esempio, utilizza i dati per dare al conducente informazioni sul traffico o sui livelli di consumo e del corretto funzionamento del veicolo.[24] Nel momento in cui vi sono due o più titolari che determinano congiuntamente finalità e mezzi del trattamento, questi sono definiti *contitolari del trattamento*:[25] essi saranno responsabili di definire i rispettivi obblighi e di comunicarli all'interessato come regolato dagli articoli 13 e 14 del GDPR, che determinano le informazioni da fornire. Tra queste si menzionano la necessità di mettere a disposizione dell'interessato l'identità e i contatti del titolare del trattamento, le finalità del trattamento, i destinatari, il periodo di

[22] GDPR Art.4, punto 1
[23] GDPR Art4, punto 7
[24] EDPB, Linee guida 01/2020 sul trattamento dei dati personali nel contesto dei veicoli connessi e delle applicazioni legate alla mobilità, Versione 2.0, adottate il 9/3/2021
[25] GDPR Art.26, punto 1

conservazione di tali dati, l'informazione dell'esistenza del diritto di accesso ai propri dati da parte dell'interessato, e così via.

- **Il responsabile del trattamento:** la persona fisica, giuridica o altro organismo che tratta i dati per conto del titolare,[26]senza che possa utilizzarli per altre finalità. Un esempio potrebbe essere quello dei costruttori di accessori o fornitori di componenti che effettuano un trattamento dei dati personali per conto del costruttore del veicolo. Il responsabile del trattamento deve rispettare gli obblighi previsti dall'articolo 28 del GDPR: non può, ad esempio, rivolgersi ad un altro responsabile senza autorizzazione scritta del titolare e comunque il trattamento da parte del responsabile deve sempre essere regolamentato da un contratto che lo vincoli alle istruzioni del titolare, definendo la natura del trattamento (vanno specificate la durata, la finalità, la tipologia di dati e gli interessati coinvolti).[27] Inoltre, vi è la necessità che il responsabile dei dati adotti tutte le misure tecniche e organizzative richieste per mantenere un elevato livello di sicurezza del trattamento, ai sensi dell'Art. 32 del GDPR: questo prevende la cifratura dei dati personali utilizzati, la capacità di assicurare la resilienza dei sistemi e dei servizi di trattamento, la rapidità nel ripristinare l'accesso ai dati in caso di eventuali incidenti e una procedura volta a verificare periodicamente l'efficacia delle misure messe in atto.[28]
- **Il destinatario:** persona fisica o organismo che riceve comunicazione di dati personali dal titolare o dal responsabile[29], ad esempio un partner commerciale di un fornitore di servizi che riceve dati generati dal veicolo.[30]

In base al Regolamento Europeo 2016/679 ogni trattamento personale deve basarsi su principi ben definiti, che mirano a tutelare i diritti degli interessanti, discussi nell'articolo 5:[31]

- **Liceità, correttezza e trasparenza** nell'utilizzo dei dati personali nei confronti degli interessati (il principio di liceità verrà approfondito di seguito);

[26] GDPR Art.4, punto 8
[27] GDPR, Artr.28, punto3
[28] GDPR, Art.32, punto 1
[29] GDPR,Art.4,punto 9
[30] EDPB, Linee guida 01/2020 sul trattamento dei dati personali nel contesto dei veicoli connessi e delle applicazioni legate alla mobilità, Versione 2.0, adottate il 9/3/2021
[31]GDPR,Art.5
https://www.privacy-regulation.eu/it/5.htm

- **Limitazione della finalità del trattamento**: i dati personali devono essere raccolti per finalità specifiche, esplicite e legittime e l'utilizzo deve essere compatibile con lo scopo per cui sono stati raccolti;
- **Minimizzazione dei dati**: i dati devono essere pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento;
- **Esattezza:** i dati devono essere esatti e aggiornati, prevedendo la cancellazione tempestiva di quelli che risultino inesatti rispetto alle finalità del trattamento;
- **Limitazione della conservazione:** i dati personali devono essere conservati per un arco di tempo non superiore a quello necessario per il conseguimento delle finalità per le quali sono stati raccolti. Ai sensi del'Art.89, paragrafo 1 del GDPR, fanno eccezione i trattamenti a fine di archiviazione nel pubblico interesse, di ricerca scientifica o storica e a fini statistici.
- **Integrità e riservatezza:** i dati devono essere trattati in modo da garantirne la sicurezza, adottando misure tecniche e organizzative adeguate per evitare accessi non autorizzati, la perdita, la distruzione o il danno accidentale.

Anche se non espressamente citato, esiste un Principio di **proporzionalità** secondo il quale il titolare deve commisurare proporzionalmente il mezzo con l'obiettivo che intende perseguire: dunque il trattamento dei dati deve essere proporzionato con l'entità del fine. Il GDPR, inoltre, non si limita a stabilire tali principi, ma impone ai titolare del trattamento anche l'onere di dimostrare di rispettarli: questo viene indicato con il principio dell' **accountability,**[32]ovvero della responsabilità, che prevede che il titolare metta in atto misure adeguate per rendere conto che il trattamento venga effettuato conformemente a quanto stabilito dal Regolamento.[33]

2.2.Liceità del trattamento

Le condizioni di liceità del trattamento vengono stabilite dall'articolo 6 del GDPR, una di queste è il consenso all'utilizzo dei dati: questo deve essere libero, specifico, informato ed inequivocabile per l'interessato. Inoltre deve essere sempre possibile revocare tale consenso in qualsiasi momento. Tra le altre fattispecie individuate che legittimano il trattamento dei dati personali vi sono l'adempimento di un obbligo contrattuale di cui l'interessato è parte, obblighi di legge, l'esercizio di funzioni di interesse pubblico, perseguimento di un interesse legittimo del titolare del trattamento

[32] GDPR,Art.5,paragrafo 2
[33] GDPR, Art 24,paragrafo 1

o di terzi. L'inosservanza del principio di liceità può comportare sanzioni amministrative, come stabilito dall'Art.83 del GDPR. L'European Data Protection Board[34] evidenzia come la mancanza di trasparenza e controllo sui dati provenienti dal veicolo connesso possa costituire una criticità rilevante per quanto riguarda la liceità del trattamento. In particolare, le problematiche individuate sono relative al fatto che conducenti e passeggeri difficilmente potranno essere adeguatamente informati circa il trattamento dei dati che avviene nel veicolo smart: in particolare perché il veicolo ha più utilizzatori che non sempre coincidono con il proprietario, il quale tendenzialmente dovrebbe avere accesso all'informativa al momento della vendita. Nella pratica diventa complesso ottenere un consenso quando gli utenti coinvolti nel trattamento all'interno del veicolo non abbiano un rapporto diretto con il proprietario, come per veicoli di seconda mano o acquistati in lising. In questo caso risulta difficile, proprio per la mancanza di informazione, dimostrare la validità del consenso, che dovrebbe essere informato. Il consenso, per come è stato definito, dovrebbe rappresentare un' inequivocabile volontà dell'interessato mentre, proprio perché il veicolo tratta spesso dati anche di soggetti diversi dal proprietario o di proprietari che si succedono, non permette una facile raccolta di un consenso specifico in base alle preferenze dei singoli utenti. Ne consegue, dunque, un consenso " di bassa qualità"[35], perché basato su un'informazione frammentaria. Il Garante Europeo ritiene dunque opportuno che l'informativa venga presentata sul computer di bordo, ma tale strumento comunque non facilita la richiesta del consenso a tutti i soggetti nel veicolo separatamente. Per le modalità di raccolta del consenso l'EDPB suggerisce l'utilizzo di icone standardizzate, con l'intento di aumentare la trasparenza e ridurre la quantità di informazioni scritte da sottoporre all'interessato.[36] In aggiunta, viene segnalato il fatto che gli interessati dovrebbero prestare il proprio consenso separatamente dall'atto di acquisto o leasing di una nuova vettura, proprio per andare ad assottigliare l'asimmetria informativa che si viene a creare lato acquirente. Risulta, dunque, una questione complessa, e ancora aperta, la possibilità di conciliare la richiesta di identificazione della persona fisica che presta consenso e la rapidità con cui questo deve avvenire all'interno del veicolo.[37]

[34] EDPB, Linee guida 01/2020 sul trattamento dei dati personali nel contesto dei veicoli connessi e delle applicazioni legate alla mobilità, Versione 2.0, adottate il 9/3/2021
[35] ibidem
[36]https://www.cybersecurity360.it/legal/privacy-dati-personali/smart-car-e-mobilita-connessa-linee-guida-per-la-sicurezza-e-il-corretto-trattamento-dei-dati/
[37] ibidem

2.3.Misure di tutela della privacy

Secondo i Garanti Europei[38], nell'ottica di rispettare il principio di minimizzazione, i costruttori del veicolo e i fornitori di servizi dovrebbero prestare particolare attenzione a raccogliere solo i dati personali pertinenti e necessari al trattamento. In questo senso vengono date alcune indicazioni pratiche: relativamente ai dati di geolocalizzazione si sottolinea che questi dovrebbero essere raccolti secondo un'adeguata frequenza di accesso e del livello di dettaglio (ad esempio non è necessario che un'applicazione del meteo acceda sempre alla geolocalizzazione del veicolo, o che oltre ad individuare la zona ne conosca sempre la posizione esatta). Inoltre, si deve comunicare all'utente che la registrazione della posizione è attiva (ad esempio tramite una spia) e comunque deve essere sempre possibile disattivarla, specificandone la finalità (qual è lo scopo di registrare la cronologia della geolocalizzazione, se questo avviene). Allo stesso modo, per i dati biometrici si sottolinea l'importanza di un sistema di riconoscimento affidabile che deve dunque avvenire tramite sensori resistenti agli attacchi, con un numero di tentativi di autentificazione limitati. Il modello biometrico deve essere memorizzato nel sistema in forma cifrata e i dati necessari per l'autentificazione dell'utente non devono essere mai archiviati. Questo richiede che gli strumenti tecnologici e il veicolo smart nella sua totalità siano progettati secondo i principi di **privacy by design e privacy by default**[39]: questi devono essere configurati in modo da garantire il rispetto della privacy degli utenti fin dal momento della progettazione tramite impostazioni predefinite che garantiscano una protezione dei dati, facilitando il rispetto degli obblighi previsti dal GDPR e promuovendo lo sviluppo di tecnologie più sicure sul tema della privacy. Quanto illustrato si concretizza in misure quali la **pseudonimizzazione**[40], che fa in modo che i dati personali non possano più essere ricondotti ad un singolo interessato senza che si faccia ricorso ad ulteriori informazioni. Questa misura è comunque reversibile e non fa venire meno la natura del dato personale né dunque l'applicazione delle relative norme del GDPR. E' comunque riconosciuta come una valida tecnica per rafforzare la sicurezza del trattamento, ancor più che spesso non sono necessari dati identificabili per il conseguimento delle finalità di un trattamento. Le linee guida suggeriscono, inoltre, l'**anonimizzazione** dei dati per quanto riguarda l'invio di dati all'esterno della vettura: questa misura è invece irreversibile e fa cessare l'attuazione dei principi di protezione dei dati a quelle che

[38]EDPB, Linee guida 01/2020 sul trattamento dei dati personali nel contesto dei veicoli connessi e delle applicazioni legate alla mobilità, Versione 2.0, adottate il 9/3/2021

[39] GDPR,Art.25

[40] GDPR,Art.4, punto5

divengono informazioni anonime, ovvero non più riferibili a persona fisica identificata o identificabile. E' vero però che a livello pratico l'anonimizzazione dei dati non è sempre di facile attuazione, come anche l'effettiva irreversibilità, soprattutto nel contesto dei veicoli smart che sono collegati a una serie di servizi e applicazioni che funzionano tramite l'accesso ad account personali che trattano dati come l'email, il nome o la data di nascita dell'utente.[41] Inoltre si segnala che i titolari del trattamento dovrebbero limitare processi che trasferiscono i dati personali all'esterno del veicolo, prediligendo invece un **trattamento locale**: questo permette di avere un maggiore controllo dell'interessato sui dati e di ridurre i rischi relativi alla cybersicurezza o di trattamenti illeciti.[42] Vengono riportate, come esempio di trattamento locale, applicazioni che permettono il trasferimento dei dati dal veicolo ai dispositivi (come il telefono) sotto il controllo dell'utente senza che vi sia la trasmissione dei dati al fornitore dell'applicazione, o applicazioni per l'attivazione di alcuni comandi tramite dati biometrici memorizzati all'interno del veicolo, o ancora applicazioni per la guida che trattano dati della modalità di guida dell'automobile per mostrare sul computer di bordo consigli per una guida ecologica. Questi costituiscono esempi di un trattamento effettuato da una persona fisica per fini esclusivamente personali, senza trasferimento di dati a un titolare o a un responsabile del trattamento, quindi tali attività esulano dall'ambito di competenza del GDPR.[43]

[41]https://www.cybersecurity360.it/legal/privacy-dati-personali/smart-car-e-mobilita-connessa-linee-guida-per-la-sicurezza-e-il-corretto-trattamento-dei-dati/

[42]EDPB, Linee guida 01/2020 sul trattamento dei dati personali nel contesto dei veicoli connessi e delle applicazioni legate alla mobilità, Versione 2.0, adottate il 9/03/2021

[43] GDPR,Art.2,punto 2

3.Assicurazioni “Pay as you drive”

Di seguito si analizza un esempio di trattamento di dati personali nel settore delle Smart Cars, introdotto dal Garante Europeo nelle Line guida 01/2020 - versione 2.0. Il caso in esame è quello delle Assicurazioni *Pay as you drive*, per le quali l’interessato stipula una polizza basata sull’uso, che prevede uno sconto del premio assicurativo a seconda di una valutazione effettuata sui chilometri percorsi e sulle abitudini di guida del conducente: questo al fine di differenziare gli utenti con uno stile di guida più sicura. Il monitoraggio di tali informazioni viene effettuato tramite un servizio telematico integrato, un’applicazione mobile o utilizzando un modulo integrato dal costruttore che registra il numero di chilometri e dati come le frenate e le accelerazioni rapide. L’elaborazione dei dati raccolti tramite il dispositivo telematico fornirà un punteggio numerico da assegnare al conducente, che quantifica il rischio a cui andrebbe incontro l’ impresa di assicurazione stipulando un’assicurazione con il soggetto in esame. L’assicurazione basata sull’uso del veicolo necessita l’espressione del consenso da parte dell’interessato, che può avvenire al momento della conclusione del contratto, ma comunque può essere sempre ritirato da parte dell’interessato. Al contraente va inoltre offerta la possibilità alternativa di scegliere una polizza non basata sull’uso, altrimenti il consenso non sarebbe più espressione della sua reale volontà. Per accedere alle informazioni archiviate nel dispositivo vale quanto illustrato dall’Art 5 della direttiva e-privacy, per il loro successivo trattamento vige invece l’Art 6 del GDPR: il fondamento giuridico di tale base si concretizza con la stipula del contratto tra interessato e impresa di assicurazione.

Si possono distinguere due tipologie di dati personali coinvolti in questo trattamento: *i dati commerciali* (sono i dati relativi alle operazioni, dati di pagamento e quelli relativi all’identificazione dell’interessato) e i *dati di utilizzo* (dati sulle modalità di guida, sulla geolocalizzazione del veicolo e dati generati dal veicolo)[44]. I dati commerciali possono essere conservati per la durata prevista dal contratto in una banca dati per poi essere archiviati su un dispositivo fisico o, altrimenti, ne può essere limitato l’accesso gestendone le autorizzazioni in modo tale da poterli consultare in caso di contenziosi. Oltre la durata stabilita tali dati devono essere eliminati o anonimizzati. I dati di utilizzo possono essere distinti in *dati grezzi*, ovvero solo le informazioni raccolte sulla condotta di guida, e *dati aggregati*, che sono stati già trattati per ottenere il risultato finale (tipicamente un punteggio che misura quanto siano buone le abitudini di guida del conducente). E’ opportuno che i dati grezzi

[44] EDPB, Linee guida 01/2020 sul trattamento dei dati personali nel contesto dei veicoli connessi e delle applicazioni legate alla mobilità, Versione 2.0, adottate il 9/03/2021

raccolti vengano trattati internamente al veicolo (dalla telematic box, o nel suo telefono) o dal fornitore di servizi telematici per conto dell'impresa assicurativa: questo permette di evitare che i titolari o i responsabili del trattamento vengano a contatto direttamente con i dati grezzi dettagliati, che devono essere separati dai dati riconducibili all'identità del conducente. Dunque, il fornitore che riceverà informazioni in tempo reale sul veicolo connesso non potrà accedere alle informazioni personali del conducente (targa, nome del proprietario...), mentre l'assicuratore potrà accede solo ai dati aggregati (quali il punteggio e il chilometraggio risultante), dal momento che è in grado di individuare l'identità dei contraenti. Laddove il trattamento dei dati grezzi è necessario al di fuori del veicolo, questi dovrebbero essere conservati solo il tempo necessario all'erogazione del servizio.

L'EDPB sottolinea che l'interessato deve essere informato prima del trattamento, in conformità con l'Art.13 del GDPR, circa il periodo di conservazione dei dati o i criteri utilizzati per determinare tale periodo e che deve essere chiara per l'utente la differenziazione tra dati grezzi e punteggi finali, per come è stata illustrata. Inoltre devono essere messi a conoscenza della profilazione, se effettuata, e della possibilità di esercitare il diritto di accesso, rettifica, limitazione e cancellazione. Vale inoltre il diritto di portabilità dei dati, previsto dall'Art. 20 del GDPR che consente all'interessato di ricevere i propri dati in un formato di uso comune e strutturato per trasmetterli ad un altro titolare del trattamento, senza che vi siano impedimenti.[45]

[45] https://www.garanteprivacy.it/documents/10160/0/Infografica+-+Diritto+alla+portabilit%25C3%25A0+dei+dati

Conclusioni

Al termine di questa analisi si ritiene, dunque, che la tematica della protezione dei dati applicata al settore dei veicoli connessi sia complessa e ancora di aperta risoluzione. Le Linee guida rilasciate dal Garante Europeo hanno richiamato l'attenzione su un tema non ancora regolamentato nel dettaglio, ma che al contempo è caratterizzato da un rapido sviluppo tecnologico e si dirige verso la guida autonoma. In particolare, si reputa rilevante il fatto che tale documento riconosca i dati raccolti e generati dal veicolo connesso come dati personali: questo auspicabilmente potrebbe sia contribuire a mutare l'approccio delle case produttrici di automobili alla gestione dei dati personali nei veicoli, sia favorire lo sviluppo di una sensibilità riguardo il tema della privacy tra i consumatori, dal momento che se ne evidenziano i rischi potenziali. Con la crescente quantità di dati da trattare nel veicolo e la complessità dei dispositivi all'interno di essi si apriranno sfide in ambito tecnologico e legislativo. Rilevanti sono, inoltre, le implicazioni etiche derivanti dallo sviluppo di software a guida autonoma. E' lecito domandarsi quali dovrebbero essere i principi sui quali progettare gli algoritmi: si può pensare un approccio utilitaristico (che tende a minimizzare il danno), uno deontologico, egoistico (che predilige sempre la salvezza del guidatore), e così via. Viene inoltre da chiedersi che mercato ci sarebbe per un'automobile che non è pensata in primis per tutelare chi l'acquista. Il settore della mobilità ha iniziato una vera e propria transizione e, affinché si riesca a trovare un equilibrio solido tra innovazione e protezione, è necessario che tutti gli stakeholder coinvolti si impegnino verso un uso dei dati personali sicuro e responsabile. D'altronde, la diffusione di questi veicoli potrebbe portare dei benefici concreti, che vanno dal miglioramento della sicurezza stradale e del livello di impatto ambientale, nuovi modelli di business e mobilità più accessibile. Si ritiene che la soluzione non possa essere tentare di arrestare un processo tecnologico ormai in fermento, quanto riuscirne a mitigarne i rischi con normative adeguate e con una progettazione del prodotto finito sempre più orientata a prevenire trattamenti dei dati personali illeciti. In questo senso il mondo scientifico, parallelamente a quello giurisprudenziale, potrebbe auspicabilmente sviluppare nuove tecnologie a tutela della privacy degli interessati.

Bibliografia

"Direttiva 2002/58/CE del Parlamento Europeo e del Consiglio" 12/07/2002, Gazzetta Ufficiale n. L 201 del 31/07/2002

"Direttiva 2008/63/CE della Commissione", 20 Giugno 2008

"Direttiva 2009/136/CE del Parlamento Europeo e del Consiglio", 25 novembre 2009

"Legge sulla Protezione dei Dati Personali", Legge n. 675, 1996

"Parere 5/2019 del Comitato Europeo per la protezione dei dati", 12/03/2019, punto 40 e 41

"Regolamento Generale sulla Protezione dei Dati (GDPR)", Regolamento EU 679/2016

"Regolamento sulla sicurezza dei veicoli", 2019/2144

"Tassonomia e definizioni relativi ai sistemi di automazione della guida per veicoli a motore su strada", Society of Automotive Engineering (SAE) J3016, 2014

"Team of Hacker take remote control of Tesla Model S from 12 miles away", The Guardian, 2016

European Data Protection Board (EDPB),"Linee guida 01/2020 sul trattamento dei dati personali nel contesto dei veicoli connessi e delle applicazioni legate alla mobilità, Versione 2.0", adottate il 9/03/2021

Ubertazzi, "Il diritto alla Privacy, Natura e funzioni giuridiche", 2004

Sitografia

Curelli, Liguori, Mandarà, "Dati anonimi e pseudonimi: cosa cambia per la ricerca dopo l'ultima sentenza della corte UE", Agenda Digitale, 7/6/2023 https://www.agendadigitale.eu/sicurezza/privacy/dati-anonimi-e-pseudonimi-cosa-cambia-per-la-ricerca-dopo-lultima-sentenza-della-corte-ue/#:~:text=5)%20GDPR%2C%20si%20ha%20pseudonimizzazione,volte%20a%20garantire%20che%20tali

"ADAS: cosa sono e quali sono i più importanti", Redazione online, 17/11/2022 https://www.alvolante.it/da_sapere/tecnica/adas-cosa-sono-e-quali-sono-piu-importanti-380565

Dimalta D., "Smart car e mobilità connessa: linee guida per la sicurezza e il corretto trattamento dei dati",Cybersecurity36

https://www.cybersecurity360.it/legal/privacy-dati-personali/smart-car-e-mobilita-connessa-linee-guida-per-la-sicurezza-e-il-corretto-trattamento-dei-dati/

Guida S., “Protezione e sicurezza dei dati personali nei veicoli connessi e nelle applicazioni per la mobilità: principi e indicazioni nelle specifiche Linee Guida del Garante europeo della privacy”, Data Protection Law, 15/04/2020

https://www.dataprotectionlaw.it/2020/04/15/protezione-e-sicurezza-dei-dati-personali-nei-veicoli-connessi-e-nelle-applicazioni-per-la-mobilita-principi-e-indicazioni-nelle-specifiche-linee-guida-del-garante-europeo-della-privacy/

Garante per la protezione dei dati personali, “Cosa intendiamo per dati personali”

https://www.garanteprivacy.it/home/diritti/cosa-intendiamo-per-dati-personali#:~:text=dati%20personali%3F*-,Cosa%20intendiamo%20per%20dati%20personali%3F*,rendono%20identificabile%20una%20persona%20fisica.

Garante per la protezione dei dati personali, “Princi fondamentali del trattamento”

https://www.garanteprivacy.it/home/principi-fondamentali-del-trattamento#:~:text=Si%20tratta%20di%20una%20delle,un%20valido%20fondamento%20di%20lic33333333333333333333333333333333333333333333333333333333333333333333333333333333333333333333333333333333333333333333333333333333333333333333333333333333333333333333333333333333333333333333333..eit%C3%A0.

“Principi applicabili al trattamento dei dati personali”; Privazyplan

https://www.privacy-regulation.eu/it/5.htm

“Smart building e Smart City, a che punto siamo: il mercato IoT in Italia”, 24/04/2024

https://www.proptech360.it/mercato/smart-building/smart-building-e-smart-city-a-che-punto-siamo-il-mercato-iot-in-italia/

Salvadori G.,“Smart Car, auto intelligenti e connesse a guida del futuro”, Osservatorio del Politecnico, di Milano, 6/12/2023

https://blog.osservatori.net/it_it/smart-car-auto-intelligenti-connesse

Garante per la protezione dei dati personali, “Il diritto alla portabilità dei dati”

https://www.garanteprivacy.it/documents/10160/0/Infografica+-+Diritto+alla+portabilit%25C3%25A0+dei+dati