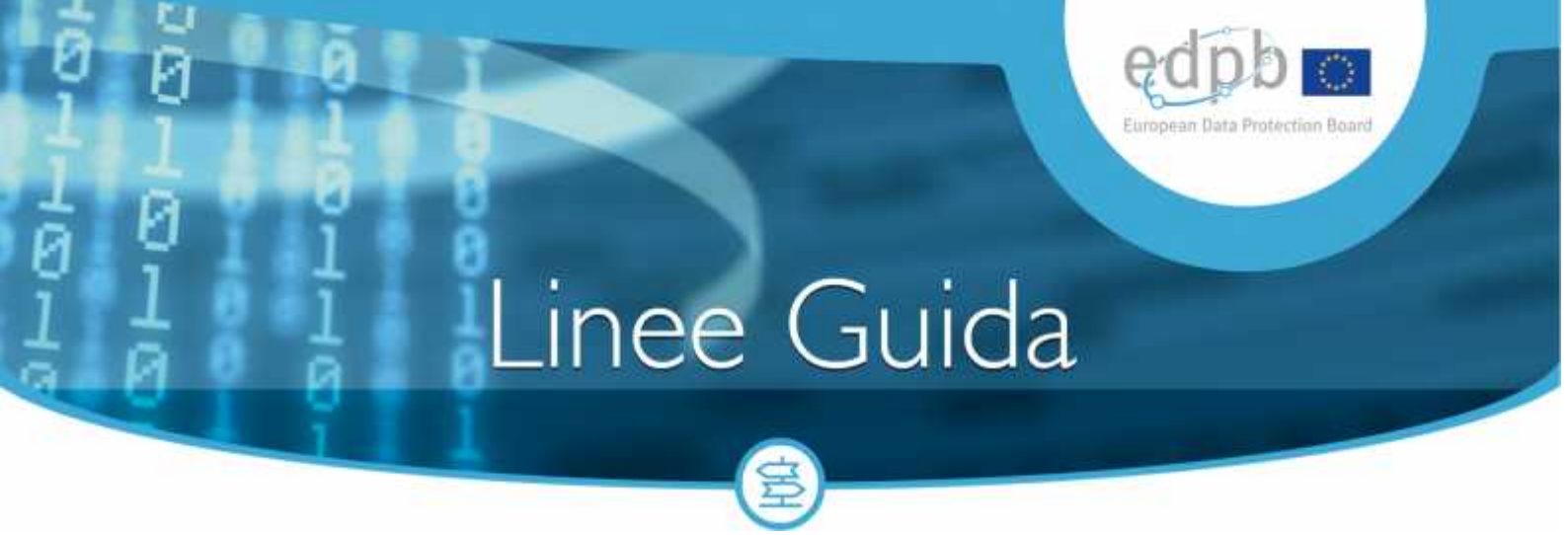

Linee guida 01/2020 sul trattamento dei dati personali nel contesto dei veicoli connessi e delle applicazioni legate alla mobilità

Versione 2.0

adottate il 9 marzo 2021

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Cronologia delle versioni

Versione 2.0	9 marzo 2021	Adozione delle linee guida dopo la consultazione pubblica
Versione 1.0	28 gennaio 2020	Adozione delle linee guida per consultazione pubblica

Indice

Il comitato europeo per la protezione dei dati,

visto l'articolo 70, paragrafo 1, lettera e), del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (di seguito "GDPR"),

visto l'accordo SEE, in particolare l'allegato XI e il protocollo 37, modificati dalla decisione del comitato misto SEE n. 154/2018 del 6 luglio 2018[1],

visti gli articoli 12 e 22 del proprio regolamento interno,

HA ADOTTATO LE SEGUENTI LINEE GUIDA

1 INTRODUZIONE

1. Simbolo dell'economia del XX secolo, l'automobile è uno dei beni di consumo di massa che hanno influenzato la società nel suo complesso. Solitamente associate al concetto di libertà, le automobili sono spesso considerate più di un semplice mezzo di trasporto. Di fatto esse rappresentano un ambito privato in cui le persone possono godere di una certa autonomia decisionale al riparo da interferenze esterne. Oggi, mentre i veicoli connessi si apprestano a diventare prodotti di largo consumo, tale visione non corrisponde più alla realtà. La connettività di bordo si sta rapidamente estendendo dai modelli di lusso e dai marchi di fascia alta ai modelli di fascia media realizzati in grandi quantità e i veicoli si stanno trasformando in enormi hub di dati. Non solo i veicoli ma anche i conducenti e i passeggeri sono sempre più connessi. Infatti molti modelli lanciati sul mercato negli ultimi anni integrano sensori e apparecchiature di bordo connesse, capaci di raccogliere e registrare, tra l'altro, le prestazioni del motore, le abitudini di guida, i luoghi visitati e, potenzialmente, persino i movimenti oculari del conducente, la frequenza cardiaca oppure dati biometrici al fine di identificare in maniera univoca una data persona fisica[2].

2. Il trattamento di questi dati avviene in un ecosistema complesso, che non è limitato agli operatori tradizionali del settore automobilistico ma è anche plasmato dall'emergere di nuovi operatori dell'economia digitale. Questi nuovi operatori potranno offrire servizi di *infotainment* quali musica online, informazioni sul traffico e sulle condizioni stradali, oppure fornire sistemi e servizi di assistenza alla guida, ad esempio software di guida autonoma, aggiornamenti sullo stato del veicolo, assicurazioni basate sull'uso (*usage-based*) o mappatura dinamica. Inoltre poiché i veicoli sono connessi tramite reti di comunicazione elettronica, anche i gestori delle infrastrutture stradali e gli operatori di telecomunicazione coinvolti in questo processo svolgono un ruolo importante per quanto riguarda le potenziali operazioni di trattamento che interessano i dati personali di conducenti e passeggeri.

3. Inoltre i veicoli connessi stanno generando crescenti quantità di dati che possono essere considerati, per la maggior parte, dati personali in quanto riferiti a conducenti o passeggeri. Anche qualora non siano direttamente correlati a un nominativo ma si riferiscano ad aspetti tecnici e a caratteristiche del veicolo, i dati raccolti da un'automobile connessa riguarderanno comunque il conducente o i passeggeri. A titolo di esempio i dati riguardanti

[1] I riferimenti agli "Stati membri" nel presente documento sono da intendersi come riferimenti agli "Stati membri del SEE".
[2] Infografica "Data and the connected car" del Future of Privacy Forum; https://fpf.org/wp-content/uploads/2017/06/2017_0627-FPF-Connected-Car-Infographic-Version-1.0.pdf.

lo stile di guida o la distanza percorsa, i dati relativi all'usura di parti del veicolo, i dati relativi all'ubicazione o quelli raccolti da videocamere possono riguardare il comportamento del conducente nonché informazioni concernenti altre persone che potrebbero trovarsi all'interno del veicolo, oppure interessati che si trovano nelle vicinanze. Tali dati tecnici sono prodotti da una persona fisica e consentono la sua identificazione diretta o indiretta da parte del titolare del trattamento o di un terzo. Il veicolo può essere considerato un terminale utilizzabile da diversi utenti. Pertanto, come accade per i personal computer, questa potenziale pluralità di utenti non influisce sulla natura personale dei dati.

4. Nel 2016 la Fédération Internationale de l'Automobile (FIA) ha organizzato una campagna a livello europeo dal titolo "My Car My Data" per sondare l'opinione dei cittadini europei riguardo alle automobili connesse[3]. La campagna ha rivelato un forte interesse dei conducenti nei confronti della connettività ma ha anche evidenziato la necessità di esercitare una sorveglianza sull'uso dei dati prodotti dai veicoli e l'importanza di ottemperare alla normativa in materia di protezione dei dati personali. Per ciascuna delle parti interessate la sfida consiste dunque nell'integrare la dimensione della "protezione dei dati personali" sin dalla fase di progettazione del prodotto e nell'offrire trasparenza agli utilizzatori di automobili oltre alla possibilità di esercitare il controllo in relazione ai loro dati come previsto al considerando 78 del GDPR. Tale approccio contribuisce a rafforzare la fiducia degli utenti e dunque lo sviluppo a lungo termine di tali tecnologie.

1.1 Lavori correlati

5. I veicoli connessi sono ampiamente diventati oggetto di regolamentazione nell'ultimo decennio, in particolare negli ultimi due anni. A livello nazionale e internazionale sono stati dunque pubblicati vari lavori in materia di sicurezza e privacy dei veicoli connessi. Tali normative e iniziative mirano a integrare con norme settoriali i quadri esistenti in materia di protezione dei dati e di tutela della vita privata o a fornire orientamenti ai professionisti.

1.1.1 Iniziative a livello europeo e internazionale

6. A decorrere dal 31 marzo 2018 un sistema eCall di bordo basato sul 112 è obbligatorio su tutti i nuovi tipi di veicoli M1 e N1 (autovetture e veicoli leggeri)[4,5]. Nel 2006 il Gruppo di lavoro Articolo 29 aveva già adottato un documento di lavoro sulle implicazioni in materia di protezione dei dati e rispetto della vita privata dell'iniziativa eCall[6]. Inoltre, come discusso in precedenza, ad ottobre del 2017 il Gruppo di lavoro Articolo 29 ha adottato un parere sul trattamento dei dati personali nel contesto dei sistemi di trasporto intelligente cooperativi (C-ITS).

7. A gennaio del 2017 l'Agenzia dell'Unione europea per la cibersicurezza (ENISA) ha pubblicato uno studio incentrato sulla cibersicurezza e sulla resilienza delle automobili intelligenti che elenca i componenti sensibili nonché le minacce, i rischi e i fattori di attenuazione corrispondenti e le possibili misure di sicurezza da attuare[7]. A settembre del 2017 la conferenza internazionale dei commissari in materia di protezione dei dati e della vita

[3] Campagna "My Car My Data", http://www.mycarmydata.eu/.
[4] The interoperable EU-wide eCall, https://ec.europa.eu/transport/themes/its/road/action_plan/ecall_en.
[5] Decisione n. 585/2014/UE del Parlamento europeo e del Consiglio, del 15 maggio 2014, sulla diffusione in tutto il territorio dell'Unione europea di un servizio elettronico di chiamata di emergenza (eCall) interoperabile (Testo rilevante ai fini del SEE), https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32014D0585.
[6] Documento di lavoro sulle implicazioni in materia di protezione dei dati e rispetto della vita privata dell'iniziativa eCall, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp125_it.pdf.
[7] "Cyber security and resilience of smart cars", https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars.

privata (ICDPPC) ha adottato una risoluzione sui veicoli connessi[8]. Infine ad aprile del 2018 anche il gruppo di lavoro internazionale sulla tutela dei dati nelle telecomunicazioni (IWGDPT) ha adottato un documento di lavoro sui veicoli connessi[9].

1.1.2 Iniziative nazionali dei membri del comitato europeo per la protezione dei dati (EDPB)

8. A gennaio del 2016 la conferenza delle autorità tedesche federali e statali per la protezione dei dati e l'associazione tedesca dell'industria automobilistica (VDA) hanno pubblicato una dichiarazione comune sui principi della protezione dei dati nei veicoli connessi e non connessi[10]. Ad agosto del 2017 il Centre for Connected and Autonomous Vehicles (CCAV) britannico ha pubblicato un documento di orientamento che stabilisce i principi della cibersicurezza per i veicoli connessi e automatizzati al fine di sensibilizzare alla questione all'interno del settore automobilistico[11]. Ad ottobre del 2017 l'autorità francese per la protezione dei dati, la Commission Nationale de l'Informatique et des Libertés (CNIL), ha pubblicato un pacchetto di conformità per le automobili connesse allo scopo di fornire alle parti interessate una serie di indicazioni su come integrare la protezione dei dati fin dalla progettazione e per impostazione predefinita in modo che gli interessati possano esercitare un controllo efficace sui dati che li riguardano[12].

1.2 Diritto applicabile

9. Il quadro giuridico dell'UE pertinente è il GDPR, che si applica in ogni caso quando il trattamento dei dati nel contesto dei veicoli connessi comporta il trattamento di dati personali di persone fisiche.

10. Oltre al GDPR, la direttiva 2002/58/CE, riveduta dalla direttiva 2009/136/CE (di seguito "direttiva e-privacy"), **definisce una norma specifica per tutti gli operatori che intendono archiviare informazioni o accedere a informazioni archiviate nell'apparecchiatura terminale di un abbonato o di un utente nello Spazio economico europeo (SEE).**

11. Di fatto sebbene la maggioranza delle disposizioni contenute nella direttiva e-privacy (articolo 6, articolo 9 ecc.) si applichi soltanto ai fornitori di servizi di comunicazione elettronica accessibili al pubblico e ai fornitori di reti pubbliche di comunicazione, l'articolo 5, paragrafo 3, della direttiva e-privacy costituisce una disposizione di carattere generale. Esso si applica non soltanto ai servizi di comunicazione elettronica ma anche a qualsiasi entità, sia essa pubblica o privata, che registri o legga informazioni sull'apparecchiatura terminale indipendentemente dalla natura dei dati che sono archiviati o a cui si accede.

12. Per quanto riguarda il concetto di "*apparecchiatura terminale*", la definizione è fornita dalla direttiva 2008/63/CE[13]. L'articolo 1, lettera a), definisce le apparecchiature terminali come "*le apparecchiature allacciate direttamente o indirettamente all'interfaccia di una rete*

[8] "Resolution on data protection in automated and connected vehicles", https://edps.europa.eu/sites/edp/files/publication/resolution-on-data-protection-in-automated-and-connected-vehicles_en_1.pdf.
[9] Documento di lavoro "Connected Vehicles", https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/working-paper/.
[10] "Data protection aspects of using connected and non-connected vehicles", https://www.lda.bayern.de/media/dsk_joint_statement_vda.pdf.
[11] Principles of cyber security for connected and automated vehicles, https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles.
[12] Pacchetto di conformità per un uso responsabile dei dati nelle automobili connesse, https://www.cnil.fr/en/connected-vehicles-compliance-package-responsible-use-data.
[13] Direttiva 2008/63/CE della Commissione, del 20 giugno 2008, relativa alla concorrenza sui mercati delle apparecchiature terminali di telecomunicazioni (Versione codificata) (Testo rilevante ai fini del SEE), https://eur-lex.europa.eu/legal-content/it/ALL/?uri=CELEX%3A32008L0063.

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 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".

13. Pertanto, a condizione che siano soddisfatti i suddetti criteri, il veicolo connesso e il dispositivo ad esso collegato dovrebbero essere considerati "*apparecchiature terminali*" (alla stregua di un computer, di uno smartphone o di una smart TV) e trovano applicazione, ove pertinente, le disposizioni dell'articolo 5, paragrafo 3, della direttiva e-privacy.

14. Come delineato dall'EDPB nel parere 5/2019 sull'interazione tra la direttiva e-privacy e il GDPR[14], l'articolo 5, paragrafo 3, della direttiva e-privacy prevede che, di norma, e fatte salve le deroghe a detta norma di cui al punto 17 in appresso, l'archiviazione di informazioni o l'accesso ad informazioni già archiviate nell'apparecchiatura terminale di un abbonato o utente richiedano il suo consenso preliminare. Nella misura in cui le informazioni archiviate nel dispositivo dell'utente finale costituiscono dati personali, l'articolo 5, paragrafo 3, della direttiva e-privacy prevale sull'articolo 6 del GDPR con riguardo alle attività di archiviazione di o accesso a tali informazioni[15]. Qualunque operazione di trattamento di dati personali successiva alle operazioni di trattamento di cui sopra, compreso il trattamento di dati personali ottenuti mediante l'accesso a informazioni nell'apparecchiatura terminale, per essere lecita deve avere un fondamento giuridico a norma dell'articolo 6 del GDPR[16].

15. Poiché, al momento di richiedere il consenso all'archiviazione delle informazioni o all'accesso alle stesse a norma dell'articolo 5, paragrafo 3, della direttiva e-privacy, il titolare del trattamento dovrà comunicare all'interessato tutte le finalità del trattamento, compreso qualsiasi trattamento successivo alle operazioni di cui sopra (ossia il "trattamento successivo"), il consenso a norma dell'articolo 6 del GDPR costituirà in genere il fondamento giuridico più adeguato su cui basare il trattamento dei dati personali successivo a dette operazioni (nella misura in cui la finalità del trattamento successivo sia compresa dall'interessato che esprime il suo consenso, cfr. i punti 53-54 in appresso). Pertanto il consenso costituirà probabilmente il fondamento giuridico sia per l'archiviazione delle informazioni e l'accesso alle informazioni già archiviate sia per il trattamento successivo di dati personali[17]. Di fatto nel valutare l'osservanza dell'articolo 6 del GDPR si dovrebbe tenere conto del fatto che il trattamento nel suo complesso comporta specifiche attività per le quali il legislatore dell'UE ha cercato di offrire un'ulteriore tutela[18]. Inoltre, nell'individuare la base legittima appropriata, i titolari del trattamento devono tenere conto dell'impatto sui diritti degli interessati in maniera da rispettare il principio di correttezza[19]. La conclusione è che 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.

---

[14] 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 autorità per la protezione dei dati, adottato il 12 marzo 2019 (di seguito "parere 5/2019"), punto 40.

[15] Ibidem, punto 40.

[16] Ibidem, punto 41.

[17] Il consenso richiesto dall'articolo 5, paragrafo 3, della direttiva "e-privacy" e il consenso necessario come fondamento giuridico per il trattamento dei dati (articolo 6 del GDPR) per la medesima finalità specifica possono essere ottenuti nello stesso momento (ad esempio mediante la selezione di una casella che indichi con chiarezza l'oggetto del consenso espresso dall'interessato).

[18] Parere 5/2019, punto 41.

[19] Comitato europeo per la protezione dei dati, Linea guida 2/2019 sul trattamento di dati personali ai sensi dell'articolo 6, paragrafo 1, lettera b), del regolamento generale sulla protezione dei dati nel contesto della fornitura di servizi online agli interessati, Versione 2.0, 8 ottobre 2019, punto 1.

16. L'EDPB ricorda che il concetto di consenso nella direttiva e-privacy corrisponde al concetto di consenso nel GDPR e deve soddisfare tutti i requisiti e le condizioni per il consenso di cui all'articolo 4, punto 11, e all'articolo 7 del GDPR.

17. Sebbene il principio fondante sia costituito dal consenso, l'articolo 5, paragrafo 3, della direttiva e-privacy consente tuttavia di esonerare l'archiviazione di informazioni o l'accesso a informazioni già archiviate nell'apparecchiatura terminale dall'obbligo del consenso informato qualora l'operazione soddisfi uno dei criteri seguenti:

- **deroga 1:** abbiano luogo al solo fine di effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica;
- **deroga 2:** abbiano luogo nella misura strettamente necessaria per consentire al fornitore di un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente di erogare tale servizio.

18. In tali casi il trattamento di dati personali, compresi i dati personali ottenuti mediante l'accesso a informazioni archiviate nell'apparecchiatura terminale, si fonda su una delle basi giuridiche fornite dall'articolo 6 del GDPR. Ad esempio il consenso non è richiesto laddove il trattamento dei dati sia necessario per fornire servizi di navigazione GPS richiesti dall'interessato qualora tali servizi siano qualificabili come servizi della società dell'informazione.

1.3 Ambito di applicazione

19. L'EDPB desidera sottolineare che le presenti linee guida intendono facilitare l'osservanza della normativa nel trattamento di dati personali effettuato da un'ampia gamma di parti interessate che operano in questo contesto. Il presente documento, tuttavia, non è finalizzato a illustrare tutti i casi d'uso possibili in tale contesto, né a fornire un orientamento per ogni possibile situazione specifica.

20. Il documento si concentra, in particolare, sul trattamento dei dati personali in relazione all'uso non professionale di veicoli connessi da parte degli interessati, ad esempio conducenti, passeggeri, proprietari di veicoli, altri utenti della strada ecc. Più specificamente il documento riguarda i dati personali: i) trattati all'interno del veicolo, ii) scambiati tra il veicolo e i dispositivi personali ad esso connessi (ad esempio lo smartphone dell'utente) oppure iii) raccolti localmente nel veicolo ed esportati verso entità esterne (ad esempio costruttori di veicoli, gestori di infrastrutture, imprese di assicurazione, officine di riparazione) ai fini di un ulteriore trattamento.

21. Nel presente documento la definizione di veicolo connesso deve essere interpretata in senso lato. Il veicolo connesso può essere definito come un veicolo dotato di numerose centraline elettroniche di controllo (ECU) collegate tra loro per mezzo di una rete di bordo, nonché di strumenti di connettività che consentono di condividere informazioni con altri dispositivi interni ed esterni al veicolo. Ciò consente lo scambio di dati tra il veicolo e i dispositivi personali ad esso collegati, ad esempio per il *mirroring* delle applicazioni mobili sull'unità di informazione e intrattenimento *in-dash* della vettura. Inoltre lo sviluppo di applicazioni mobili *stand-alone*, ossia indipendenti dal veicolo (ad esempio basate esclusivamente sull'utilizzo dello smartphone), che forniscono assistenza ai conducenti, rientra nell'oggetto del presente documento, in quanto tali applicazioni contribuiscono a determinare le capacità di connettività del veicolo anche qualora, di fatto, non si basino di per sé sullo scambio di dati con il veicolo stesso. Le applicazioni per i veicoli connessi sono molteplici e diversificate. Di seguito se ne forniscono alcuni esempi[20].

[20] PwC Strategy 2014. "In the fast lane. The bright future of connected cars", https://www.strategyand.pwc.com/media/file/Strategyand_In-the-Fast-Lane.pdf.

22. *Gestione della mobilità:* funzioni che consentono ai conducenti di raggiungere la destinazione in tempi brevi e in maniera efficiente sul piano dei costi, fornendo informazioni tempestive riguardanti la navigazione GPS, la presenza di condizioni ambientali potenzialmente pericolose (ad esempio ghiaccio sulle strade), la congestione del traffico o la presenza di lavori stradali, parcheggi o autofficine, il consumo ottimizzato del carburante o i pedaggi stradali.

23. *Gestione del veicolo:* funzioni pensate per aiutare i conducenti a ridurre i costi d'esercizio e a migliorare la facilità di utilizzo, ad esempio avvisi sullo stato del veicolo e avvisi di manutenzione programmata, trasferimento dei dati relativi all'utilizzo (ad esempio per i servizi di riparazione del veicolo), assicurazioni personalizzate di tipo "*Pay As/How You Drive*", operazioni a distanza (ad esempio impianto di riscaldamento) o configurazioni del profilo (ad esempio posizione dei sedili).

24. *Sicurezza stradale:* funzioni che avvisano il conducente riguardo a pericoli esterni e risposte interne, ad esempio protezione in caso di collisione, avvisi di pericolo, avvisi di deviazione dalla corsia di marcia, rilevamento della stanchezza del conducente, chiamata d'emergenza (eCall) o "scatole nere" (registratori di dati relativi ad eventi incidentali) utilizzate a fini di indagine.

25. *Intrattenimento:* funzioni che forniscono informazioni e offrono intrattenimento al conducente e ai passeggeri, ad esempio interfacce con gli smartphone (chiamate telefoniche a mani libere, SMS vocali), hotspot WLAN, musica, video, internet, social media, servizi di *mobile office* o servizi di "domotica".

26. *Assistenza alla guida:* funzioni che comportano l'automazione parziale o totale della guida, ad esempio assistenza operativa o guida autonoma in presenza di traffico intenso, nelle manovre di parcheggio o sulle autostrade.

27. *Benessere:* funzioni che monitorano il comfort del conducente, la sua capacità di guidare e la sua idoneità alla guida, come ad esempio il rilevamento della stanchezza o l'assistenza medica.

28. Pertanto i veicoli possono nascere già connessi o no e i dati personali possono essere raccolti con mezzi diversi, ossia: i) sensori di bordo, ii) *telematic box* o iii) applicazioni mobili (ad esempio accessibili da un dispositivo appartenente al conducente). Per rientrare nell'ambito di applicazione del presente documento le applicazioni mobili devono essere correlate all'ambiente di guida. Ad esempio le applicazioni di navigazione GPS rientrano nell'ambito del presente documento. Sono invece escluse dall'ambito delle presenti linee guida le applicazioni le cui funzionalità si limitano a suggerire ai conducenti luoghi di interesse (ristoranti, monumenti storici ecc.).

29. Molti dei dati generati da un veicolo connesso riguardano persone fisiche identificate o identificabili e pertanto costituiscono dati personali. Ad esempio i dati comprendono dati identificabili direttamente (come l'identità completa del conducente) e dati identificabili indirettamente, quali informazioni dettagliate sui viaggi effettuati, i dati sull'utilizzo del veicolo (riguardanti, ad esempio, lo stile di guida o la distanza percorsa) o i dati tecnici del veicolo (ad esempio dati relativi all'usura di parti del veicolo), che, messi in relazione con altri dati e soprattutto con il numero di identificazione del veicolo (VIN), possono permettere di risalire a una persona fisica. I dati personali nei veicoli connessi possono comprendere anche metadati, ad esempio dati relativi allo stato di manutenzione del veicolo. In altri termini qualunque dato associabile a una persona fisica rientra quindi nell'ambito di applicazione del presente documento.

30. L'ecosistema del veicolo connesso comprende un'ampia gamma di parti interessate. Più precisamente tale ecosistema comprende operatori tradizionali del settore automobilistico

e operatori emergenti del settore digitale. Le presenti linee guida sono pertanto rivolte ai costruttori di veicoli, ai costruttori di accessori e ai fornitori di componenti, ai riparatori di autoveicoli, alle concessionarie automobilistiche, ai fornitori di servizi automobilistici, ai gestori di parchi veicoli, alle compagnie di assicurazione dei veicoli a motore, ai fornitori di servizi di intrattenimento, agli operatori di telecomunicazioni, ai gestori di infrastrutture stradali e alle amministrazioni pubbliche, nonché agli interessati. L'EDPB sottolinea che le categorie di interessati saranno diverse da un servizio all'altro (ad esempio conducenti, proprietari, passeggeri ecc.). Il suddetto elenco non è esaustivo, in quanto l'ecosistema è costituito da una vasta gamma di servizi, che comprende servizi per i quali è necessaria l'autenticazione o l'identificazione diretta e servizi per i quali tale autenticazione o identificazione non è richiesta.

31. Alcuni trattamenti di dati da parte di persone fisiche all'interno del veicolo sono effettuati "*per l'esercizio di attività a carattere esclusivamente personale o domestico*" e di conseguenza sono esclusi dall'ambito di applicazione del GDPR[21]. Ciò riguarda, in particolare, l'uso esclusivo di dati personali all'interno del veicolo da parte degli interessati che li hanno trasmessi al quadro strumenti del veicolo. Tuttavia l'EDPB ricorda che, conformemente al considerando 18, il GDPR "*si applica ai titolari del trattamento o ai responsabili del trattamento che forniscono i mezzi per trattare dati personali nell'ambito di tali attività a carattere personale o domestico*".

1.3.1 Quali operazioni non rientrano nell'ambito di applicazione del presente documento

32. I datori di lavoro che forniscono autovetture aziendali ai loro dipendenti potrebbero decidere di monitorare le azioni dei dipendenti (ad esempio per garantire la sicurezza del dipendente, delle merci o dei veicoli, per assegnare risorse, per tenere traccia di un servizio e addebitarne il costo o per controllare le ore di lavoro). Il trattamento di dati effettuato dai datori di lavoro in tale contesto solleva considerazioni che attengono specificamente all'ambito dei rapporti di lavoro e che potrebbero essere disciplinate da normative del lavoro a livello nazionale sulle quali le presenti linee guida non possono soffermarsi[22].

33. Anche se il trattamento di dati nel contesto dei veicoli commerciali destinati all'uso professionale (ad esempio trasporto pubblico), dei trasporti condivisi e della soluzione MaaS (Mobility-as-a-Service) potrebbero sollevare considerazioni specifiche che esulano dall'ambito di applicazione delle presenti linee guida generali, molti dei principi e delle raccomandazioni formulati nel presente documento saranno applicabili anche a tali tipologie di trattamento.

34. Poiché sono sistemi abilitati alla connessione radio, i veicoli connessi sono soggetti al tracciamento passivo, ad esempio al tracciamento Wi-Fi o Bluetooth. In tal senso non differiscono da altri dispositivi connessi e rientrano nell'ambito di applicazione della direttiva e-privacy, che è attualmente in fase di revisione. Ne consegue che è esclusa dall'ambito del presente documento anche la localizzazione su vasta scala di veicoli dotati di connessione Wi-Fi[23] da parte di una fitta rete di persone che transitano o sostano in prossimità del veicolo e che utilizzano i comuni servizi di posizione degli smartphone. Tali servizi comunicano regolarmente ai server centrali tutte le reti Wi-Fi visibili. Poiché il Wi-Fi

[21] Cfr. l'articolo 2, paragrafo 2, lettera c), del GDPR.
[22] Il Gruppo di lavoro Articolo 29 si è espresso a tale riguardo nel parere 2/2017 sul trattamento dei dati sul posto di lavoro (WP249), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169.
[23] Per maggiori informazioni cfr. https://www.datenschutzzentrum.de/artikel/1269-Location-Services-can-Systematically-Track-Vehicles-with-WiFi-Access-Points-at-Large-Scale.html.

integrato può essere considerato un identificativo secondario del veicolo[24], vi è il rischio di una raccolta sistematica e continuativa dei profili completi degli spostamenti dei veicoli.

35. Sempre più spesso i veicoli sono dotati di dispositivi per la registrazione di immagini (ad esempio telecamere di assistenza al parcheggio o *dashcam*). Poiché ciò si ricollega al problema della ripresa di luoghi pubblici, che esige una valutazione del quadro legislativo pertinente, specifico di ciascuno Stato membro, questo trattamento di dati non rientra nell'ambito di applicazione delle presenti linee guida.

36. Il trattamento di dati nel contesto dei sistemi di trasporto intelligenti cooperativi (C-ITS), quali definiti nella direttiva 2010/40/UE[25], è stato oggetto di un parere specifico del Gruppo di lavoro Articolo 29[26]. Sebbene la definizione del concetto di C-ITS nella direttiva non contenga specifiche tecniche, nel suo parere il Gruppo di lavoro Articolo 29 si concentra sulle comunicazioni a corto raggio, ossia quelle che non comportano l'intervento di un operatore di rete. Più specificamente esso fornisce un'analisi per casi di utilizzo specifici per la diffusione iniziale e si è impegnato a valutare in una fase successiva le nuove questioni che certamente sorgeranno con l'attuazione di livelli di automazione più elevati. Poiché le implicazioni per la protezione dei dati nel contesto del C-ITS sono molto specifiche (quantitativi di dati senza precedenti sull'ubicazione, trasmissione continua di dati personali, scambio di dati tra veicoli e altre infrastrutture di trasporto ecc.) e che il tema è tuttora oggetto di discussione a livello europeo, il trattamento di dati personali in tale contesto esula dall'ambito di applicazione delle presenti linee guida.

37. Infine il presente documento non mira ad affrontare tutte le possibili questioni e i possibili interrogativi sollevati dai veicoli connessi e non può essere pertanto considerato esaustivo.

1.4 Definizioni

38. Il **trattamento** di dati personali comprende qualsiasi operazione che riguardi dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione ecc.[27].

39. L'**interessato** è la persona fisica a cui si riferiscono i dati che sono oggetto di trattamento. Nel contesto dei veicoli connessi potrà trattarsi, in particolare, del conducente (principale o occasionale), del passeggero o del proprietario del veicolo[28].

40. Il **titolare del trattamento** è la persona che determina le finalità e i mezzi del trattamento che ha luogo nei veicoli connessi[29]. I titolari del trattamento possono essere i fornitori di servizi che trattano i dati del veicolo per trasmettere al conducente informazioni sul traffico,

---

[24] Markus Ullmann, Tobias Franz, and Gerd Nolden, Vehicle Identification Based on Secondary Vehicle Identifier -- Analysis, and Measurements, in Proceedings, VEHICULAR 2017, The Sixth International Conference on Advances in Vehicular Systems, Technologies and Applications, Nice, France, July 23 to 27, 2017, pagg. 32-37.

[25] Direttiva 2010/40/UE del Parlamento europeo e del Consiglio, del 7 luglio 2010, sul quadro generale per la diffusione dei sistemi di trasporto intelligenti nel settore del trasporto stradale e nelle interfacce con altri modi di trasporto, https://eur-lex.europa.eu/legal-content/it/TXT/PDF/?uri=CELEX:32010L0040.

[26] Gruppo di lavoro Articolo 29 - Parere 03/2017 sul documento intitolato "Trattamento dei dati personali nel contesto del sistema di trasporto intelligente cooperativo (C-ITS)", http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610171.

[27] Cfr. l'articolo 4, punto 2, del GDPR.

[28] Cfr. l'articolo 4, punto 1, del GDPR.

[29] Cfr. l'articolo 4, punto 7, del GDPR e il documento del comitato europeo per la protezione dei dati dal titolo Guidelines 07/2020 on the concepts of controller and processor in the GDPR (di seguito "Linee guida 07/2020").

messaggi relativi alla guida ecologica o avvisi sul funzionamento del veicolo, oppure imprese di assicurazione che offrono contratti a consumo di tipo "*Pay As You Drive*" o costruttori di veicoli che raccolgono dati sull'usura di parti del veicolo per migliorarne la qualità. A norma dell'articolo 26 del GDPR due o più titolari possono determinare congiuntamente le finalità e i mezzi del trattamento ed essere pertanto considerati contitolari del trattamento. In tal caso essi devono definire con chiarezza i rispettivi obblighi, con particolare riguardo all'esercizio dei diritti degli interessati e alla comunicazione delle informazioni di cui agli articoli 13 e 14 del GDPR.

41. Il **responsabile del trattamento** è chiunque tratti dati personali in nome e per conto del titolare del trattamento[30]. Il responsabile del trattamento raccoglie e tratta i dati secondo le istruzioni del titolare del trattamento, senza utilizzare tali dati per i propri scopi. A titolo di esempio in alcuni casi è possibile che i costruttori di accessori e i fornitori di componenti trattino dati per conto dei costruttori di veicoli (il che non implica che non possano essere titolari del trattamento per altre finalità). Oltre a stabilire che i responsabili del trattamento devono mettere in atto misure tecniche e organizzative adeguate in modo tale da garantire un livello di sicurezza adattato al rischio, l'articolo 28 del GDPR definisce gli obblighi dei responsabili del trattamento.

42. Per **destinatario** si intende la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi[31]. A titolo di esempio un partner commerciale del fornitore di servizi che riceva da quest'ultimo dati personali generati dal veicolo è destinatario di dati personali e, indipendentemente dal fatto che funga da nuovo titolare del trattamento o da responsabile del trattamento, è tenuto ad adempiere tutti gli obblighi imposti dal GDPR.

43. Tuttavia le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari[32]; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento. Ad esempio le autorità di contrasto sono terzi autorizzati quando richiedono dati personali nell'ambito di un'indagine conformemente al diritto dell'Unione o degli Stati membri.

[30] Cfr. l'articolo 4, punto 8, del GDPR e le linee guida 07/2020.
[31] Cfr. l'articolo 4, punto 9, del GDPR e le linee guida 07/2020.
[32] Articolo 4, punto 9, e considerando 31 del GDPR.

1.5 Rischi relativi alla tutela della vita privata e alla protezione dei dati

44. Il Gruppo di lavoro Articolo 29 ha già espresso diverse preoccupazioni in merito ai sistemi internet degli oggetti (*Internet of Things* - IoT) che possono essere estese anche ai veicoli connessi[33]. I problemi relativi alla sicurezza e al controllo dei dati, già sottolineati in relazione all'IoT, sono ancora più cruciali nel contesto dei veicoli connessi, giacché attengono a questioni di sicurezza stradale (e possono avere un impatto sull'integrità fisica del conducente) in un contesto tradizionalmente percepito come isolato e protetto da interferenze esterne.

45. Inoltre i veicoli connessi sollevano serie preoccupazioni per la tutela della vita privata e la protezione dei dati per quanto concerne il trattamento di dati relativi all'ubicazione, in quanto il carattere sempre più invasivo di questo trattamento può mettere a dura prova le attuali possibilità di mantenere l'anonimato. L'EDPB desidera porre un particolare accento e sensibilizzare le parti interessate sul fatto che l'utilizzo di tecnologie di localizzazione esige l'introduzione di specifiche tutele al fine di impedire la sorveglianza delle persone e l'abuso dei dati.

1.5.1 Mancanza di controllo e asimmetria dell'informazione

46. I conducenti e i passeggeri dei veicoli potrebbero non essere sempre adeguatamente informati in merito al trattamento dei dati che ha luogo all'interno o per mezzo di un veicolo connesso. È possibile che le informazioni siano fornite soltanto al proprietario del veicolo, che potrebbe non essere il conducente, e che inoltre non siano fornite in maniera tempestiva. Esiste dunque il rischio che le funzionalità o le opzioni offerte non siano sufficienti per esercitare il controllo necessario affinché le persone interessate possano avvalersi del loro diritto al rispetto della vita privata e alla protezione dei dati. Si tratta di un aspetto importante in quanto, nel corso della loro vita utile, i veicoli potrebbero appartenere a più di un proprietario perché sono venduti o perché, anziché essere acquistati, sono acquisiti in leasing.

47. Inoltre la comunicazione nel veicolo può essere avviata automaticamente e tramite impostazioni predefinite, senza che il diretto interessato ne sia al corrente. In assenza della possibilità di controllare efficacemente l'interazione tra il veicolo e le apparecchiature ad esso connesse, il controllo del flusso di dati da parte dell'utente è destinato a diventare estremamente difficile. Sarà ancora più difficile controllarne l'uso successivo per evitare un potenziale "slittamento della funzione" *(function creep*).

1.5.2 Qualità del consenso dell'utente

48. L'EDPB sottolinea che, laddove il trattamento dei dati sia basato sul consenso, devono essere rispettati tutti gli elementi del consenso valido; ciò significa che il consenso deve essere libero, specifico e informato e costituisce una manifestazione di volontà inequivocabile dell'interessato, secondo l'interpretazione fornita nelle linee guida dell'EDPB sul consenso[34]. I titolari del trattamento devono prestare molta attenzione alle modalità di ottenimento del consenso valido presso i vari partecipanti, quali i proprietari o gli utilizzatori di autovetture. Tale consenso deve essere prestato separatamente, per finalità specifiche e non può essere accorpato al contratto di acquisto o leasing di una nuova autovettura. Il consenso deve poter essere revocato con la stessa facilità con cui lo si è espresso.

49. Lo stesso principio deve essere applicato quando il consenso è necessario per ottemperare alla direttiva e-privacy, ad esempio in caso di archiviazione di informazioni o di accesso a informazioni già archiviate nel veicolo, come previsto in taluni casi dall'articolo 5,

[33] 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.
[34] Comitato europeo per la protezione dei dati, Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679, Versione 1.1, 4 maggio 2020 (di seguito "linee guida 5/2020").

paragrafo 3, di tale direttiva. Infatti, come sottolineato sopra, in tale contesto il consenso deve essere interpretato alla luce del GDPR.

50. In molti casi l'utente potrebbe non essere consapevole del trattamento dei dati effettuato nel suo veicolo. Tale mancanza di informazione costituisce un ostacolo rilevante quando si tratta di dimostrare la validità del consenso ai sensi del GDPR, giacché il consenso deve essere informato. In tali circostanze il consenso non può essere utilizzato come base giuridica per il corrispondente trattamento dei dati a norma del GDPR.

51. I meccanismi classici usati per ottenere il consenso delle persone possono essere difficili da applicare nel contesto dei veicoli connessi. Pertanto si ottiene un consenso "di bassa qualità", basato su una mancanza di informazione o sull'impossibilità di fatto di prestare un consenso ben calibrato che tenga conto delle preferenze espresse dalle persone. Nella pratica il consenso può essere difficile da ottenere anche laddove i conducenti e passeggeri non siano collegati al proprietario del veicolo, nel caso di veicoli di seconda mano, acquisiti in leasing, noleggiati o presi in prestito.

52. Nei casi in cui la direttiva e-privacy non richiede il consenso dell'interessato, il titolare del trattamento ha comunque la responsabilità di scegliere, ai sensi dell'articolo 6 del GDPR, il fondamento giuridico più adatto al caso per il trattamento dei dati personali.

1.5.3 Ulteriore trattamento di dati personali

53. Quando sono raccolti sulla base del consenso a norma dell'articolo 5, paragrafo 3, della direttiva e-privacy o sulla base di una delle deroghe di cui all'articolo 5, paragrafo 3 e sono successivamente trattati conformemente all'articolo 6 del GDPR, i dati possono essere sottoposti a un ulteriore trattamento soltanto se il titolare del trattamento richiede un ulteriore consenso per tale finalità diversa o è in grado di dimostrare che il trattamento è basato su un atto legislativo dell'Unione o degli Stati membri per la salvaguardia degli obiettivi di cui all'articolo 23, paragrafo 1, del GDPR[35]. L'EDPB ritiene che l'ulteriore trattamento sulla base della verifica di compatibilità ai sensi dell'articolo 6, paragrafo 4, del GDPR non sia possibile in tali casi, in quanto pregiudicherebbe il livello di protezione dei dati offerto dalla direttiva e-privacy. Infatti il consenso, ove previsto dalla direttiva e-privacy, deve essere specifico e informato; ciò significa che gli interessati devono essere al corrente della finalità di ciascun trattamento di dati e avere il diritto di rifiutare finalità specifiche[36]. Il fatto di ritenere possibile l'ulteriore trattamento sulla base di una verifica di compatibilità ai sensi dell'articolo 6, paragrafo 4, del GDPR eluderebbe il principio stesso dei requisiti del consenso stabiliti dalla direttiva vigente.

54. L'EDPB ricorda che il consenso iniziale non legittimerà mai l'ulteriore trattamento, in quanto il consenso è valido solo se informato e specifico.

55. Ad esempio i dati di telemetria, che sono raccolti durante l'utilizzo del veicolo a scopo di manutenzione, non possono essere comunicati alle compagnie di assicurazione dei veicoli a motore senza il consenso degli utenti ai fini della creazione di profili di conducenti finalizzata all'offerta di polizze di assicurazione basate sulla condotta di guida.

56. Inoltre i dati raccolti dai veicoli connessi possono essere trattati dalle autorità di contrasto per rilevare violazioni dei limiti di velocità o altre infrazioni se e quando sono soddisfatte le condizioni specifiche della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie. In questo caso tali dati saranno considerati relativi a condanne penali e reati in base alle condizioni stabilite dall'articolo 10 del GDPR e della legislazione nazionale eventualmente applicabile. I costruttori possono fornire tali dati alle autorità di contrasto

[35] Cfr. anche comitato europeo per la protezione dei dati, Guidelines 10/2020 on restrictions under Article 23 GDPR**.**

[36] Linee guida 5/2020, sezioni 3.2 e 3.3.

qualora siano soddisfatte le condizioni specifiche per tale trattamento. L'EDPB sottolinea che il trattamento di dati personali effettuato al solo scopo di soddisfare le richieste delle autorità di contrasto non costituisce una finalità determinata, esplicita e legittima ai sensi dell'articolo 5, paragrafo 1, lettera b), del GDPR. Quando sono autorizzate dalla legge, le autorità di contrasto potrebbero costituire "terzi" ai sensi dell'articolo 4, punto 10, del GDPR; in questo caso i costruttori sarebbero autorizzati a trasmettere loro i dati di cui dispongono nel rispetto delle disposizioni di legge pertinenti di ciascuno Stato membro.

1.5.4 Raccolta eccessiva di dati

57. Il continuo aumento del numero di sensori integrati nei veicoli connessi comporta il rischio assai elevato di una raccolta eccessiva di dati rispetto a quella necessaria allo scopo.

58. Lo sviluppo di nuove funzionalità, più specificamente quelle basate su algoritmi di apprendimento automatico (*machine learning*), potrebbe rendere necessaria la raccolta di una grande quantità di dati per un periodo di tempo prolungato.

1.5.5 Sicurezza dei dati personali

59. L'ampia gamma di funzionalità, servizi e interfacce (ad esempio web, USB, RFID, Wi-Fi) offerta dai veicoli connessi aumenta la superficie di attacco e dunque il numero di vulnerabilità potenziali attraverso cui i dati personali potrebbero essere compromessi. A differenza della maggioranza dei dispositivi IoT, i veicoli connessi sono sistemi critici in cui una violazione della sicurezza potrebbe mettere a repentaglio la vita degli utilizzatori e delle persone che si trovano nelle vicinanze. È dunque ancora più importante affrontare il rischio rappresentato dalla possibilità che gli hacker tentino di sfruttare le vulnerabilità dei veicoli connessi.

60. Inoltre i dati personali memorizzati nei veicoli e/o in luoghi esterni (ad esempio le infrastrutture di *cloud computing*) devono essere adeguatamente protetti dall'accesso non autorizzato. Ad esempio durante un intervento di manutenzione il veicolo sarà affidato a un meccanico che avrà bisogno di accedere ad alcuni dati tecnici. Il meccanico deve poter accedere ai dati tecnici ma potrebbe tentare di accedere a tutti i dati memorizzati nel veicolo.

2 RACCOMANDAZIONI GENERALI

61. Al fine di attenuare i suddetti rischi per gli interessati, si formulano in appresso alcune raccomandazioni di carattere generale rivolte ai costruttori di veicoli e di accessori, ai fornitori di servizi e ad ogni altra parte interessata che agisca in qualità di titolare del trattamento o di responsabile del trattamento in relazione ai veicoli connessi.

2.1 Categorie di dati

62. Come osservato nell'introduzione, i dati associati ai veicoli connessi saranno per la maggior parte considerati dati personali nella misura in cui sono ricollegabili ad una o più persone identificabili. Ciò vale anche per i dati tecnici relativi agli spostamenti del veicolo (ad esempio velocità o distanza percorsa) e allo stato del veicolo (ad esempio temperatura del liquido di raffreddamento del motore, regime del motore, pressione degli pneumatici). Taluni dati generati dai veicoli connessi potrebbero meritare particolare attenzione anche per via della loro sensibilità e/o del loro potenziale impatto sui diritti e sugli interessi degli interessati. Attualmente l'EDPB ha individuato tre categorie di dati personali su cui i costruttori di veicoli e accessori, i fornitori di servizi e altri titolari del trattamento dovrebbero porre particolare attenzione: dati relativi all'ubicazione, dati biometrici (e qualsiasi categoria particolare di dati di cui all'articolo 9 del GDPR) e dati che potrebbero rivelare reati o violazioni del codice della strada.

2.1.1 Dati relativi all'ubicazione

63. Nella raccolta di dati personali i costruttori di veicoli e accessori, i fornitori di servizi e altri titolari del trattamento dovrebbero tenere presente che i dati relativi all'ubicazione sono particolarmente atti a fornire indicazioni sulle abitudini di vita degli interessati. I viaggi effettuati hanno la particolare caratteristica di permettere di risalire al luogo di lavoro e di residenza, nonché ai centri di interesse (svago) del conducente e possono eventualmente rivelare informazioni sensibili quali il credo religioso attraverso il luogo di culto, oppure l'orientamento sessuale sulla base dei luoghi visitati. Pertanto i costruttori di veicoli e accessori, i fornitori di servizi e altri titolari del trattamento dovrebbero avere cura di non raccogliere dati relativi all'ubicazione tranne qualora ciò sia assolutamente necessario per la finalità del trattamento. A titolo di esempio laddove il trattamento consista nel rilevare gli spostamenti del veicolo il giroscopio è sufficiente allo scopo e non è necessario raccogliere dati relativi all'ubicazione.

64. In generale la raccolta di dati relativi all'ubicazione deve osservare anche i principi seguenti:

- configurazione adeguata della frequenza di accesso ai dati relativi all'ubicazione, e del loro livello di dettaglio, in relazione alla finalità del trattamento. Ad esempio un'applicazione per le previsioni del tempo non dovrebbe essere in grado di accedere ogni secondo alla posizione del veicolo, nemmeno qualora l'interessato abbia espresso il proprio consenso;
- comunicazione di informazioni accurate sulla finalità del trattamento (ad esempio la cronologia delle posizioni è conservata? Se lo è, a che scopo?);
- quando il trattamento è basato sul consenso, ottenimento di un consenso valido (libero, specifico e informato) che sia distinto dalle condizioni generali di vendita o di utilizzo, ad esempio sul computer di bordo;
- attivazione della posizione non per impostazione predefinita e in maniera continuativa dal momento dell'avvio della vettura ma soltanto quando l'utente attiva una funzionalità che richiede la posizione del veicolo;
- comunicazione all'utente del fatto che la posizione è stata attivata, in particolare mediante l'utilizzo di icone (ad esempio una freccia che si sposta sul display);
- possibilità di disattivare la posizione in qualsiasi momento;
- definizione di un periodo di conservazione limitato.

2.1.2 Dati biometrici

65. Nel contesto dei veicoli connessi i dati biometrici utilizzati al fine di identificare in modo univoco una persona fisica possono essere trattati, tra l'altro, limitatamente a quanto previsto dall'articolo 9 del GDPR e in base alle deroghe nazionali, per consentire l'accesso a un veicolo, l'autenticazione del conducente/proprietario e/o l'accesso alle impostazioni del profilo e alle preferenze del conducente. Nel valutare il possibile utilizzo di dati biometrici, al fine di garantire all'interessato il pieno controllo sui dati che lo riguardano è necessario, da un lato, prevedere l'esistenza di un'alternativa non biometrica (ad esempio l'utilizzo di una chiave o di un codice) senza ulteriori vincoli (in altri termini l'uso di dati biometrici non dovrebbe essere obbligatorio) e, dall'altro lato, conservare e confrontare il modello biometrico in forma cifrata solo a livello locale, senza che i dati biometrici siano trattati da un terminale di lettura/raffronto esterno.

66. Nel caso dei dati biometrici[37] è importante garantire che la soluzione di autenticazione biometrica sia sufficientemente affidabile, in particolare rispettando i principi seguenti:

[37] Il principio di divieto di cui all'articolo 9, paragrafo 1, del GDPR riguarda esclusivamente i "*dati biometrici intesi a identificare in modo univoco una persona fisica*".

- l'adeguamento della soluzione biometrica utilizzata (ad esempio il tasso di falsi positivi e falsi negativi) è funzionale al livello di sicurezza del controllo degli accessi richiesto;
- la soluzione biometrica utilizzata si basa su un sensore resistente agli attacchi (ad esempio utilizzo di impronte piane per il riconoscimento delle impronte digitali);
- il numero di tentativi di autenticazione è limitato;
- il modello biometrico è memorizzato nel veicolo in forma cifrata utilizzando un algoritmo crittografico e una gestione delle chiavi adeguati allo stato dell'arte;
- i dati grezzi utilizzati per l'elaborazione del modello biometrico e per l'autenticazione dell'utente sono trattati in tempo reale senza mai essere archiviati, neppure localmente.

2.1.3 Dati che rivelano reati o altre violazioni

67. Ai fini del trattamento di dati relativi a reati potenziali ai sensi dell'articolo 10 del GDPR l'EDPB raccomanda di ricorrere al trattamento locale dei dati, sul quale l'interessato ha il pieno controllo (cfr. le considerazioni relative al trattamento locale nella sezione 2.4). In realtà, fatte salve alcune eccezioni (cfr. lo studio di caso relativo agli studi sull'incidentalità illustrato nella sezione 3.3), il trattamento esterno di dati che rivelano reati o altre violazioni è vietato. Pertanto in base alla sensibilità dei dati è necessario porre in essere misure di sicurezza efficaci come quelle descritte nella sezione 2.7, al fine di offrire una protezione contro l'accesso, la modifica e la cancellazione illegittimi di tali dati.

68. Effettivamente alcune categorie di dati personali provenienti dai veicoli connessi potrebbero rivelare che è stato commesso o è in corso un reato o un altro tipo di violazione ("dati relativi ai reati") e pertanto potrebbero essere soggette a particolari restrizioni (ad esempio dati indicanti che il veicolo ha oltrepassato una linea bianca, dati relativi alla velocità istantanea di un veicolo combinati con dati sulla posizione esatta). In particolare qualora tali dati siano trattati dalle autorità nazionali competenti a fini di indagine penale e perseguimento di reati, si applicherebbero le garanzie previste all'articolo 10 del GDPR.

2.2 Finalità

69. I dati personali possono essere trattati per una vasta gamma di finalità in relazione ai veicoli connessi, tra cui la sicurezza del conducente, l'assicurazione, il trasporto efficiente, l'intrattenimento o i servizi di informazione. Conformemente al GDPR i titolari del trattamento devono garantire che le loro finalità siano "determinate, esplicite e legittime", che i dati siano successivamente trattati in un modo che non sia incompatibile con tali finalità e che vi sia una valida base giuridica per il trattamento secondo quanto previsto all'articolo 5 del GDPR. Alcuni esempi concreti di finalità perseguite dai titolari del trattamento che operano nel contesto dei veicoli connessi sono illustrati nella parte III delle presenti linee guida, in cui sono inoltre formulate raccomandazioni specifiche per ciascuna tipologia di trattamento.

2.3 Pertinenza e minimizzazione dei dati

70. Al fine di rispettare il principio della minimizzazione dei dati[38] i costruttori di veicoli e accessori, i fornitori di servizi e altri titolari del trattamento dovrebbero prestare particolare attenzione alle categorie di dati che essi hanno la necessità di ottenere da un veicolo connesso, giacché sono tenuti a raccogliere soltanto dati personali pertinenti e necessari al trattamento. Ad esempio i dati relativi all'ubicazione sono particolarmente invasivi e possono rivelare molte delle abitudini di vita degli interessati. Pertanto gli operatori del settore dovrebbero avere particolare cura di evitare la raccolta di dati relativi all'ubicazione

[38] Articolo 5, paragrafo 1, lettera c), del GDPR.

tranne qualora essa sia assolutamente necessaria rispetto alla finalità del trattamento (cfr. la sezione 2.1. e le considerazioni ivi contenute riguardo ai dati relativi all'ubicazione).

2.4 Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

71. Tenuto conto del volume e della varietà dei dati personali generati dai veicoli connessi, l'EDPB rileva che i titolari del trattamento sono tenuti a garantire che le tecnologie utilizzate nel contesto dei veicoli connessi siano configurate in maniera tale da rispettare la vita privata delle persone applicando gli obblighi in materia di protezione dei dati fin dalla progettazione e per impostazione predefinita di cui all'articolo 25 del GDPR. Le tecnologie dovrebbero essere progettate in modo tale da minimizzare la raccolta di dati personali, fornire impostazioni predefinite a tutela della vita privata e garantire che gli interessati siano correttamente informati e abbiano la possibilità di modificare agevolmente le configurazioni associate ai loro dati personali. A beneficio del settore e dei fornitori terzi di applicazioni potrebbe essere utile fornire orientamenti specifici sulle modalità con cui i costruttori e i fornitori di servizi possono adempiere gli obblighi in materia di protezione dei dati fin dalla progettazione e per impostazione predefinita.

72. Talune pratiche generali, descritte in appresso, possono anch'esse contribuire a ridurre i rischi per i diritti e le libertà delle persone fisiche associati ai veicoli connessi[39].

2.4.1 Trattamento locale di dati personali

73. In generale i costruttori di veicoli e accessori, i fornitori di servizi e altri titolari del trattamento dovrebbero, ogni qual volta possibile, utilizzare processi che non prevedano l'uso di dati personali o il trasferimento di dati personali all'esterno del veicolo (ossia i dati dovrebbero essere trattati internamente). Tuttavia, per loro stessa natura, i veicoli connessi presentano di fatto alcuni rischi, ad esempio la possibilità di attacchi al trattamento locale da parte di soggetti esterni o fughe di dati locali mediante la vendita di parti del veicolo. È dunque opportuno prestare particolare attenzione e prevedere l'adozione di misure di sicurezza adeguate per garantire che i dati continuino ad essere trattati solo localmente. Tale scenario offre il vantaggio di garantire all'utente il pieno ed esclusivo controllo dei dati personali che lo riguardano e, per tale ragione, presenta, "fin dalla progettazione", meno rischi per la tutela della vita privata soprattutto perché vieta alle parti interessate di effettuare il trattamento all'insaputa dell'interessato. Esso consente inoltre il trattamento di dati sensibili, quali dati biometrici o dati relativi a reati o altre violazioni, nonché di dati dettagliati relativi all'ubicazione che sarebbe altrimenti soggetto a norme più stringenti (cfr. in appresso). Analogamente tale approccio presenta minori rischi per la cibersicurezza e comporta una minore latenza, il che lo rende particolarmente indicato per le funzioni di assistenza alla guida automatizzata. Di seguito si forniscono alcuni esempi di questo tipo di soluzione:

- applicazioni di guida ecologica che trattano dati nel veicolo per mostrare in tempo reale sul display di bordo consigli in materia di guida ecologica;

- applicazioni che comportano il trasferimento di dati personali a un dispositivo come ad esempio uno smartphone sotto il pieno controllo dell'utente (ad esempio tramite Bluetooth o Wi-Fi) e nelle quali i dati del veicolo non sono trasmessi al fornitore dell'applicazione o al costruttore del veicolo; un esempio potrebbe essere costituito dall'associazione dello smartphone per l'utilizzo del display della vettura, dei sistemi multimediali, del microfono (o di altri sensori) per le telefonate ecc., nella misura in cui i dati raccolti rimangano sotto il

[39] Cfr. anche comitato europeo per la protezione dei dati, Linee guida 4/2019 sull'articolo 25 - Protezione dei dati fin dalla progettazione e per impostazione predefinita, Versione 2.0, adottate il 20 ottobre 2020 (di seguito "linee guida 4/2019").

controllo dell'interessato e siano utilizzati esclusivamente per fornire il servizio da questi richiesto;

- applicazioni di bordo per il miglioramento della sicurezza, ad esempio quelle che prevedono la trasmissione di segnali acustici o di vibrazioni del volante quando il conducente sorpassa una vettura senza azionare la freccia o supera una linea bianca, o che forniscono avvisi sullo stato del veicolo (ad esempio sull'usura delle pastiglie dei freni);

- applicazioni per lo sblocco, l'avvio e/o l'attivazione di determinati comandi del veicolo mediante i dati biometrici del conducente memorizzati all'interno del veicolo (ad esempio modelli facciali o vocali o particolarità delle impronte digitali).

74. Applicazioni come quelle suindicate comportano un trattamento effettuato da una persona fisica per l'esercizio di attività a carattere esclusivamente personale (ossia senza il trasferimento di dati personali a un titolare del trattamento o a un responsabile del trattamento). In conformità con l'articolo 2, paragrafo 2, del GDPR, **tali applicazioni esulano pertanto dall'ambito di applicazione del GDPR.**

75. Tuttavia, sebbene il GDPR non si applichi ai trattamenti di dati personali effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico, conformemente al suo considerando 18 esso si applica invece ai titolari del trattamento o ai responsabili del trattamento che forniscono i mezzi per trattare dati personali nell'ambito di tali attività a carattere personale o domestico (costruttori automobilistici, fornitori di servizi ecc.). Quando agiscono in qualità di titolari del trattamento o di responsabili del trattamento, tali soggetti devono pertanto sviluppare un'applicazione di bordo sicura nel rispetto del principio di tutela della vita privata fin dalla progettazione e per impostazione predefinita. Ad ogni modo conformemente al considerando 78 del GDPR "*(i)n fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati*"[40]. Da un lato questo processo migliorerà lo sviluppo di servizi incentrati sull'utente e, dall'altro lato, faciliterà e consentirà in futuro eventuali utilizzi successivi che potrebbero rientrare nell'ambito di applicazione del GDPR. Più specificamente l'EDPB raccomanda di sviluppare una piattaforma applicativa di bordo sicura, fisicamente separata dalle funzioni della vettura legate alla sicurezza, affinché l'accesso ai dati del veicolo non dipenda da capacità *cloud* esterne non necessarie.

76. Ogni qual volta possibile i costruttori di autovetture e i fornitori di servizi dovrebbero prendere in considerazione la possibilità di un trattamento locale dei dati al fine di attenuare i rischi potenziali del trattamento in *cloud*, quali delineati nel parere sul *cloud computing* del Gruppo di lavoro Articolo 29[41].

77. In generale gli utenti dovrebbero essere in grado di controllare la modalità con cui i propri dati sono raccolti e trattati all'interno del veicolo:

- le informazioni relative al trattamento devono essere fornite nella lingua del conducente (manuale, impostazioni ecc.);

[40] Per ulteriori raccomandazioni in materia di tutela della vita privata fin dalla progettazione e per impostazione predefinita, cfr. anche le linee guida 4/2019.
[41] Gruppo di lavoro Articolo 29 – Parere 05/2012 sul *cloud computing*, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_it.pdf.

- l'EDPB raccomanda di sottoporre a trattamento per impostazione predefinita soltanto i dati strettamente necessari al funzionamento del veicolo. Gli interessati dovrebbero avere la possibilità di attivare o disattivare il trattamento dei dati per ogni altra finalità e da parte di ogni altro titolare/responsabile del trattamento e avere la possibilità di cancellare i dati in questione, tenendo conto della finalità e della base giuridica del trattamento;
- i dati non dovrebbero essere trasmessi a terzi (ossia l'utente ha accesso esclusivo ai dati);
- i dati dovrebbero essere conservati soltanto per il periodo di tempo necessario alla prestazione del servizio o come altrimenti previsto dal diritto dell'Unione o degli Stati membri;
- gli interessati dovrebbero essere in grado di cancellare definitivamente qualsiasi dato personale prima che i veicoli siano messi in vendita;
- gli interessati dovrebbero, ove fattibile, avere un accesso diretto ai dati generati da tali applicazioni.

78. Infine, sebbene non sia sempre possibile ricorrere al trattamento locale per ogni caso d'uso, spesso potrà essere predisposto un "trattamento ibrido". Ad esempio, nel contesto dell'assicurazione basata sull'uso, i dati personali relativi alla condotta di guida (ad esempio la forza esercitata sul pedale del freno, il chilometraggio percorso ecc.) potrebbero essere trattati all'interno del veicolo oppure dal fornitore di servizi telematici per conto dell'impresa di assicurazione (il titolare del trattamento) per generare punteggi numerici da trasmettere a quest'ultima con una frequenza prestabilita (ad esempio su base mensile). In tal modo l'impresa di assicurazione non avrà accesso ai dati grezzi sulla condotta di guida ma potrà accedere soltanto al punteggio aggregato, che è il risultato del trattamento. Il rispetto del principio di minimizzazione dei dati è così garantito sin dalla progettazione. Ciò significa anche che gli utenti devono avere la possibilità di esercitare il loro diritto quando i dati sono conservati da altri soggetti: ad esempio l'utente dovrebbe avere la possibilità di cancellare i dati conservati nei sistemi di un'officina di riparazione o di una concessionaria alle condizioni stabilite dall'articolo 17 del GDPR.

2.4.2 Anonimizzazione e pseudonimizzazione

79. Qualora sia prevista la trasmissione di dati personali all'esterno del veicolo, sarebbe opportuno valutare la possibilità di renderli anonimi prima della loro trasmissione. In fase di anonimizzazione il titolare del trattamento dovrebbe tenere conto di tutti i trattamenti che potrebbero potenzialmente condurre alla re-identificazione dei dati, ad esempio la trasmissione di dati anonimizzati localmente. L'EDPB ricorda che i principi di protezione dei dati non si applicano alle informazioni anonime, vale a dire alle informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato[42]. Una volta che un insieme di dati è reso effettivamente anonimo e le persone non sono più identificabili, le norme europee in materia di protezione dei dati non sono più applicabili. Pertanto l'anonimizzazione, ove pertinente, potrebbe costituire una strategia valida per preservare i vantaggi e attenuare i rischi relativi ai veicoli connessi.

80. Come precisato nel parere del Gruppo di lavoro Articolo 29 sulle tecniche di anonimizzazione, per conseguire l'anonimizzazione dei dati si possono utilizzare vari metodi, talvolta in combinazione tra loro[43].

[42] Cfr. l'articolo 4, punto 1, e il considerando 26 del GDPR.
[43] Gruppo di lavoro Articolo 29 - Parere 05/2014 sulle tecniche di anonimizzazione, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_it.pdf.

81. Altre tecniche come ad esempio la pseudonimizzazione[44] possono contribuire a ridurre i rischi generati dal trattamento dei dati, tenendo conto che, nella maggioranza dei casi, per conseguire la finalità del trattamento non sono necessari dati direttamente identificabili. La pseudonimizzazione, se rafforzata da garanzie di sicurezza, migliora la protezione dei dati personali riducendo i rischi di abuso. A differenza dell'anonimizzazione, la pseudonimizzazione è reversibile e i dati pseudonimizzati sono considerati dati personali soggetti al GDPR.

2.4.3 Valutazioni d'impatto sulla protezione dei dati

82. Alla luce della portata e della sensibilità dei dati personali che possono essere generati *attraverso* i veicoli connessi è probabile che il trattamento, soprattutto in situazioni nelle quali i dati personali sono trattati all'esterno del veicolo, determini spesso un rischio elevato per i diritti e le libertà delle persone. In tali casi gli operatori del settore saranno tenuti a effettuare una valutazione d'impatto sulla protezione dei dati al fine di individuare e attenuare i rischi secondo quanto previsto agli articoli 35 e 36 del GDPR. Anche laddove la valutazione d'impatto sulla protezione dei dati non sia necessaria, è buona prassi effettuarne una quanto prima nella fase di progettazione. Ciò consentirà agli operatori del settore di integrare i risultati di tale analisi nelle rispettive scelte di progettazione prima della diffusione di nuove tecnologie.

2.5 Informazione

83. Prima del trattamento dei dati personali, sono fornite all'interessato informazioni riguardanti l'identità del titolare del trattamento (ad esempio il costruttore di veicoli e accessori o il fornitore di servizi), la finalità del trattamento, i destinatari dei dati, il periodo di conservazione dei dati e i diritti dell'interessato a norma del GDPR[45].

84. Inoltre il costruttore di veicoli e accessori, il fornitore di servizi o un altro titolare del trattamento dovrebbero anche fornire all'interessato, in termini chiari, semplici e facilmente accessibili, le informazioni seguenti:

- i dati di contatto del responsabile della protezione dei dati;
- le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
- il riferimento esplicito ai legittimi interessi perseguiti dal titolare del trattamento o da terzi qualora tali legittimi interessi costituiscano la base giuridica del trattamento;
- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;

[44] Articolo 4, punto 5, del GDPR. Relazione dell'Enisa del 3 dicembre 2019, https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices.
[45] Articolo 5, paragrafo 1, lettera a), e articolo 13 del GDPR. Cfr. anche il documento del Gruppo di lavoro Articolo 29 Linee guida sulla trasparenza ai sensi del regolamento 2016/679 (wp260rev.01), approvato dall'EDPB.

- l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca qualora il trattamento sia basato sul consenso;
- ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e il riferimento alle garanzie utilizzate per il trasferimento;
- se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione, che produca effetti giuridici che riguardano l'interessato o che incida in modo analogo significativamente sulla sua persona, e informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato. Un tipico esempio potrebbe essere costituito dalla fornitura di polizze di assicurazione basate sull'uso alle persone fisiche;
- il diritto di proporre reclamo a un'autorità di controllo;
- informazioni relative all'ulteriore trattamento;
- in caso di contitolarità del trattamento, informazioni chiare e complete sulle responsabilità di ciascun titolare del trattamento.

85. In alcuni casi i dati personali non sono raccolti direttamente presso l'interessato. Ad esempio un costruttore di veicoli e accessori potrebbe affidare a un concessionario la raccolta di informazioni sul proprietario del veicolo in modo tale da offrire un servizio di assistenza stradale di emergenza. Quando la raccolta dei dati non è diretta, il costruttore di veicoli e accessori, il fornitore di servizi o un altro titolare del trattamento, oltre a fornire le informazioni di cui sopra, deve indicare le categorie di dati personali interessati, la provenienza dei dati personali e, se del caso, specificare se tali dati provengono da fonti pubblicamente disponibili. Il titolare del trattamento deve fornire tali informazioni entro un termine ragionevole dall'ottenimento dei dati e **non oltre la prima delle date seguenti** conformemente all'articolo 14, paragrafo 3, del GDPR: i) entro un mese dall'ottenimento dei dati, in considerazione delle specifiche circostanze in cui i dati personali sono trattati, ii) al momento della prima comunicazione all'interessato, oppure iii) se i dati sono trasmessi a un terzo, prima della trasmissione.

86. Potrà inoltre essere necessario fornire nuove informazioni agli interessati nel caso in cui subentri un nuovo titolare del trattamento. Un servizio di assistenza stradale che interagisce con veicoli connessi può essere fornito da diversi titolari del trattamento a seconda del paese o della regione in cui è richiesta l'assistenza. I nuovi titolari del trattamento dovrebbero fornire agli interessati le informazioni necessarie quando questi ultimi si spostano da un paese all'altro e i servizi che interagiscono con i veicoli connessi sono forniti da nuovi titolari del trattamento.

87. Le informazioni possono essere fornite agli interessati in maniera stratificata[46], ossia separando due livelli di informazioni: da un lato le informazioni di primo livello, che sono le più importanti per gli interessati e, dall'altro lato, le informazioni che si presume siano di interesse in una fase successiva. Le informazioni essenziali di primo livello comprendono, oltre all'identità del titolare del trattamento, la finalità del trattamento e una descrizione dei diritti dell'interessato, così come qualsiasi altra informazione sul trattamento che ha il maggiore impatto sull'interessato e sul trattamento che potrebbe coglierlo di sorpresa. Per

[46] Cfr. il documento del Gruppo di lavoro Articolo 29 Linee guida sulla trasparenza ai sensi del regolamento 2016/679 (wp260rev.01), approvato dall'EDPB.

i veicoli connessi l'EDPB raccomanda che l'interessato sia informato di tutti i destinatari col primo strato di informazioni. Come indicato dal Gruppo di lavoro Articolo 29 nelle linee guida sulla trasparenza, i titolari del trattamento dovrebbero fornire sui destinatari le informazioni più pregnanti per gli interessati. In pratica si tratterà solitamente dei nomi dei destinatari, in maniera tale che gli interessati sappiano con precisione chi è in possesso dei dati personali che li riguardano. Se i titolari del trattamento non sono in grado di fornire i nomi dei destinatari, le informazioni dovrebbero essere il più specifiche possibile e indicare il tipo di destinatario (ad esempio facendo riferimento alle attività svolte), l'ambito di attività, il settore, il comparto e la sede dei destinatari.

88. Gli interessati potrebbero essere informati mediante clausole concise e facilmente comprensibili contenute nel contratto di vendita del veicolo, nel contratto di prestazione di servizi e/o in qualsiasi supporto scritto, utilizzando documenti distinti (ad esempio il manuale o il libretto di manutenzione del veicolo) oppure il computer di bordo.

89. In aggiunta alle informazioni necessarie si potrebbe fare ricorso a icone standardizzate, secondo quanto previsto dagli articoli 13 e 14 del GDPR, al fine di aumentare la trasparenza riducendo potenzialmente la necessità di presentare all'interessato grandi quantità di informazioni scritte. Le icone dovrebbero essere visibili nei veicoli in modo tale da fornire, in maniera comprensibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto. L'EDPB sottolinea l'importanza di standardizzare le icone, affinché l'utente ritrovi gli stessi simboli indipendentemente dalla marca o dal modello del veicolo. Ad esempio quando sono raccolte determinate tipologie di dati, ad esempio dati relativi all'ubicazione, i veicoli potrebbero essere dotati di un chiaro segnale a bordo (ad esempio una spia all'interno del veicolo) che informi i passeggeri della raccolta di dati.

2.6 Diritti dell'interessato

90. I costruttori di veicoli e accessori, i fornitori di servizi e altri titolari del trattamento dovrebbero agevolare l'esercizio, da parte degli interessati, del controllo sui propri dati durante l'intero periodo del trattamento, attraverso l'attuazione di strumenti specifici che consentano agli interessati di esercitare efficacemente i loro diritti, in particolare il diritto di accesso, di rettifica, di cancellazione, il diritto di limitazione di trattamento e, a seconda della base giuridica del trattamento, il diritto alla portabilità dei dati e il diritto di opposizione.

91. Per facilitare le modifiche delle impostazioni sarebbe opportuno attivare un sistema di gestione dei profili al fine di memorizzare le preferenze dei conducenti noti e aiutarli a modificare facilmente, in qualsiasi momento, le rispettive impostazioni sulla privacy. Il sistema di gestione dei profili dovrebbe centralizzare ogni impostazione dei dati per ciascun trattamento, soprattutto per facilitare l'accesso, la cancellazione, l'eliminazione e la portabilità dei dati personali provenienti dai sistemi del veicolo su richiesta dell'interessato. I conducenti dovrebbero avere la possibilità di bloccare temporaneamente o definitivamente, in qualsiasi momento, la raccolta di determinate tipologie di dati, salvo qualora il titolare del trattamento sia autorizzato a proseguire la raccolta di determinati dati sulla base di uno specifico fondamento giuridico. Nel caso di contratti che prevedono un'offerta personalizzata in base alla condotta di guida, ciò potrebbe comportare per l'utente il conseguente ripristino delle condizioni contrattuali standard. Tali funzionalità dovrebbero essere disponibili all'interno del veicolo ma potrebbero essere messe a disposizione degli interessati anche attraverso altri mezzi (ad esempio un'applicazione dedicata). Inoltre per consentire agli interessati di eliminare rapidamente e con facilità dati personali che possono essere memorizzati nel quadro strumenti della vettura (ad esempio cronologia della navigazione GPS, navigazione sul web ecc.) l'EDPB raccomanda ai costruttori di fornire una funzionalità semplice (ad esempio un pulsante di cancellazione).

92. Anche la vendita di un veicolo connesso e il conseguente passaggio di proprietà dovrebbero determinare la cancellazione di eventuali dati personali che non sono più necessari per le

finalità specifiche precedenti e l'interessato dovrebbe essere in grado di esercitare il suo diritto alla portabilità.

2.7 Sicurezza

93. I costruttori di veicoli e accessori, i fornitori di servizi e altri titolari del trattamento dovrebbero porre in essere misure atte a garantire la sicurezza e la riservatezza dei dati trattati e adottare tutte le precauzioni utili ad impedire che una persona non autorizzata acquisisca il controllo dei dati. In particolare gli operatori del settore dovrebbero prendere in considerazione la possibilità di adottare le misure seguenti:

- cifratura dei canali di comunicazione per mezzo di un algoritmo conforme allo stato dell'arte;
- messa a punto di un sistema di gestione delle chiavi di cifratura che sia univoco per veicolo e non per modello;
- laddove i dati siano conservati a distanza, cifratura mediante algoritmi conformi allo stato dell'arte;
- aggiornamento periodico delle chiavi di cifratura;
- protezione delle chiavi di cifratura dalla possibile divulgazione;
- autenticazione dei dispositivi di ricezione di dati;
- misure atte a garantire l'integrità dei dati (ad esempio mediante *hashing*);
- tecniche di autenticazione utente affidabili per l'accesso ai dati personali (password, certificato elettronico ecc.).

94. Per quanto riguarda, più specificamente, i costruttori di veicoli, l'EDPB raccomanda di attuare le misure di sicurezza seguenti:

- separazione delle funzioni vitali del veicolo da quelle che si basano costantemente sulle capacità di telecomunicazione (ad esempio "*infotainment*");
- attuazione di misure tecniche che consentano ai costruttori di veicoli di correggere rapidamente le vulnerabilità per la sicurezza durante la vita utile del veicolo;
- per quanto riguarda le funzioni vitali del veicolo, utilizzo prioritario, nei limiti del possibile, di mezzi di comunicazione sicuri specificamente dedicati al trasporto;
- creazione di un sistema di allarme in caso di attacco ai sistemi del veicolo, con la possibilità di attivare l'esercizio in modalità degradata[47];
- conservazione della cronologia degli accessi al sistema informatico del veicolo, ad esempio limitata ai sei mesi precedenti, per consentire di capire l'origine di un potenziale attacco e di eseguire periodicamente un esame delle informazioni registrate in modo da individuare eventuali anomalie.

95. Queste raccomandazioni generali dovrebbero essere integrate da requisiti specifici che tengano conto delle caratteristiche e della finalità di ciascun trattamento.

2.8 Trasferimento di dati personali a terzi

96. In linea di massima soltanto il titolare del trattamento e l'interessato hanno accesso ai dati generati da un veicolo connesso. Il titolare del trattamento può tuttavia trasmettere dati

[47] La modalità degradata è una modalità di esercizio che garantisce le funzioni essenziali per l'utilizzo in sicurezza del veicolo (ad esempio requisiti minimi di sicurezza), nonostante la disattivazione di altre funzionalità meno importanti (ad esempio il funzionamento del dispositivo di geoguida può essere considerato non essenziale, a differenza dell'impianto frenante).

personali a un partner commerciale (destinatario), nella misura in cui tale trasmissione si fondi lecitamente su una delle basi giuridiche di cui all'articolo 6 del GDPR.

97. Considerata la possibile sensibilità dei dati sull'uso del veicolo (ad esempio viaggi effettuati, stile di guida), l'EDPB raccomanda di ottenere sistematicamente il consenso dell'interessato prima di trasmettere i suoi dati a un partner commerciale che agisca in qualità di titolare del trattamento (ad esempio mediante la selezione di una casella non preselezionata oppure, ove tecnicamente fattibile, utilizzando un dispositivo fisico o logico a cui la persona possa accedere dal veicolo). Il partner commerciale diventa, a sua volta, responsabile dei dati che riceve ed è soggetto a tutte le disposizioni del GDPR.

98. Il costruttore del veicolo, il fornitore di servizi o un altro titolare del trattamento può trasmettere dati personali a un responsabile del trattamento che interverrà nella prestazione del servizio all'interessato, fermo restando che il responsabile del trattamento non può utilizzare tali dati per i propri scopi. I titolari del trattamento e i responsabili del trattamento sono tenuti a redigere un contratto o un altro atto giuridico che specifichi gli obblighi di ciascuna parte e richiami le disposizioni dell'articolo 28 del GDPR.

2.9 Trasferimento di dati personali al di fuori dell'UE/del SEE

99. Quando i dati personali sono trasferiti al di fuori dello Spazio economico europeo sono previste speciali garanzie per assicurare che il trasferimento avvenga in condizioni di sicurezza.

100. Di conseguenza il titolare del trattamento può trasferire dati personali a un destinatario soltanto nella misura in cui tale trasferimento abbia luogo in conformità con i requisiti di cui al capo V del GDPR.

2.10 Uso di tecnologie Wi-Fi di bordo

101. I progressi compiuti nel campo della tecnologia cellulare hanno reso possibile l'utilizzo agevole di internet in viaggio. Oltre alla connettività Wi-Fi disponibile nel veicolo attraverso l'hotspot di uno smartphone o un dispositivo dedicato (dongle OBD-II, router o modem wireless ecc.), oggi la maggioranza dei costruttori offre modelli che includono una connessione dati cellulare integrata e sono anche in grado di creare reti Wi-Fi. A seconda dei casi si dovranno prendere in considerazione vari aspetti:

- la connettività Wi-Fi è offerta come servizio da un operatore del trasporto stradale, ad esempio da un tassista ai suoi clienti. In questo caso il professionista o la sua azienda potrebbe essere considerato un fornitore di servizi internet (ISP) e come tale essere soggetto a particolari obblighi e restrizioni riguardo al trattamento dei dati personali dei suoi clienti;

- la connettività Wi-Fi è ad uso esclusivo del conducente (non è disponibile per i passeggeri). In tal caso il trattamento dei dati personali è considerato un'attività a carattere esclusivamente personale o domestico ai sensi dell'articolo 2, paragrafo 2, lettera c), e del considerando 18 del GDPR.

102. In generale il proliferare di interfacce di connessione a internet tramite Wi-Fi presenta maggiori rischi per la tutela della vita privata delle persone. In effetti attraverso i loro veicoli gli utenti diventano emittenti continui e possono pertanto essere identificati e localizzati. Al fine di impedire la localizzazione i costruttori di veicoli e accessori dovrebbero quindi predisporre opzioni "*opt-out*" di facile utilizzo atte a impedire il rilevamento dell'identificativo del servizio di rete (*Service Set Identifier* o SSID) della rete Wi-Fi di bordo.

3 STUDI DI CASI

103. La presente sezione illustra cinque esempi specifici di trattamento nel contesto dei veicoli connessi, corrispondenti ad altrettanti scenari che potrebbero configurarsi per le parti interessate del settore. Gli esempi riguardano trattamenti che richiedono una potenza di calcolo non erogabile localmente nel veicolo e/o il trasferimento di dati personali a un soggetto terzo per l'esecuzione di un'ulteriore analisi o la fornitura di ulteriori funzionalità a distanza. Per ciascuna tipologia di trattamento il presente documento specifica le finalità previste, le categorie di dati raccolti, il periodo di conservazione di tali dati, i diritti degli interessati, le misure di sicurezza da attuare e i destinatari delle informazioni. Qualora alcuni di questi aspetti non siano illustrati nel prosieguo del documento, valgono le raccomandazioni generali formulate nelle sezioni precedenti.

104. Gli esempi prescelti non sono esaustivi e intendono fornire un'indicazione della varietà di tipologie di trattamento, di basi giuridiche, di soggetti ecc. che possono intervenire nel contesto dei veicoli connessi.

3.1 Prestazione di un servizio da parte di un terzo

105. Gli interessati possono stipulare un contratto con un fornitore di servizi per ricevere servizi a valore aggiunto relativi al proprio veicolo. Ad esempio l'interessato potrebbe stipulare una polizza di assicurazione basata sull'uso che preveda uno sconto del premio assicurativo in funzione del chilometraggio percorso ("Pay As You Drive") o della buona condotta di guida ("Pay How You Drive") e che richieda il monitoraggio delle abitudini di guida da parte dell'impresa di assicurazione. L'interessato potrebbe anche stipulare con una società un contratto che offra assistenza stradale in caso di guasto e che comporti la comunicazione della posizione del veicolo alla società, oppure con un fornitore di servizi per la ricezione di messaggi o avvisi relativi al funzionamento del veicolo (ad esempio avvisi sullo stato di usura dei freni o avvisi di manutenzione).

3.1.1 Assicurazione basata sull'uso

106. L'assicurazione "Pay as You Drive" è una tipologia di assicurazione basata sull'uso che tiene traccia del chilometraggio percorso dal conducente e/o delle sue abitudini di guida per differenziare e ricompensare i conducenti che guidano in condizioni di "sicurezza" offrendo loro tariffe di premio scontate. L'assicuratore inviterà il conducente a installare un servizio telematico integrato, un'applicazione mobile o ad attivare un modulo integrato dal costruttore che tiene traccia dei chilometri percorsi e/o della condotta di guida (frenate, accelerazione rapida ecc.) del contraente. Le informazioni raccolte dal dispositivo telematico saranno utilizzate per assegnare al conducente un punteggio al fine di esaminare quali rischi potrebbe presentare per l'impresa di assicurazione.

107. Poiché l'assicurazione basata sull'uso esige il consenso a norma dell'articolo 5, paragrafo 3, della direttiva e-privacy, l'EDPB sottolinea che il contraente deve avere la possibilità di scegliere una polizza di assicurazione non basata sull'uso. Se così non fosse il consenso non sarebbe considerato liberamente prestato, giacché l'esecuzione del contratto sarebbe condizionata alla prestazione del consenso. Inoltre l'articolo 7, paragrafo 3, del GDPR stabilisce che l'interessato ha il diritto di revocare il consenso.

3.1.1.1 Base giuridica

108. Quando i dati sono raccolti attraverso un servizio di comunicazione elettronica accessibile al pubblico (ad esempio *attraverso* la scheda SIM contenuta nel dispositivo telematico), sarà necessario ottenere il consenso per potere accedere a informazioni già archiviate nel veicolo come previsto dall'articolo 5, paragrafo 3, della direttiva e-privacy. In questo contesto, infatti, non è applicabile nessuna delle deroghe previste dalle suddette disposizioni: il trattamento non è eseguito al solo fine di effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica né riguarda un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente. Il consenso potrebbe essere ottenuto al momento della conclusione del contratto.

109. Per quanto riguarda il trattamento di dati personali dopo la registrazione sull'apparecchiatura terminale dell'utente finale o l'accesso alla stessa, l'impresa di assicurazione può invocare l'articolo 6, paragrafo 1, lettera b), del GDPR in questo specifico contesto, a condizione che sia in grado di stabilire che il trattamento ha luogo nell'ambito di un contratto valido concluso con l'interessato e che è necessario all'esecuzione di tale contratto. Nella misura in cui il trattamento è oggettivamente necessario per l'esecuzione del contratto concluso con l'interessato, l'EDPB ritiene che l'applicazione dell'articolo 6, paragrafo 1, lettera b), del GDPR non avrebbe per effetto di ridurre l'ulteriore tutela offerta dall'articolo 5, paragrafo 3, della direttiva e-privacy in questo caso specifico. Tale fondamento giuridico è rappresentato dalla stipula, da parte dell'interessato, del contratto con l'impresa di assicurazione.

3.1.1.2 Dati raccolti

110. I dati personali di cui tenere conto sono di due tipi:

- **dati commerciali e dati relativi alle operazioni**: informazioni di identificazione dell'interessato, dati relativi alle operazioni, dati relativi ai mezzi di pagamento ecc.;
- **dati di utilizzo**: dati personali generati dal veicolo, abitudini di guida, posizione ecc.

111. L'EDPB raccomanda che, nella misura del possibile e considerato il rischio che i dati raccolti tramite la *telematic box* possano essere utilizzati impropriamente per creare un profilo esatto degli spostamenti del conducente, i dati grezzi relativi alla condotta di guida siano trattati:

- all'interno del veicolo nelle *telematic box* o nello smartphone dell'utente, in modo tale che l'assicuratore abbia accesso soltanto ai dati dei risultati (ad esempio un punteggio relativo alle abitudini di guida) e non ai dati grezzi dettagliati (cfr. la sezione 2.1);

- oppure dal fornitore di servizi telematici per conto del titolare del trattamento (l'impresa di assicurazione) per generare punteggi numerici che saranno trasferiti all'impresa di assicurazione con una frequenza prestabilita. In questo caso i dati grezzi devono essere separati dai dati direttamente riferiti all'identità del conducente. Ciò significa che il fornitore di servizi telematici riceve i dati in tempo reale ma ignora i nomi, le targhe e altre informazioni dei contraenti. Dall'altro lato l'assicuratore conosce i nomi dei contraenti ma riceve soltanto i punteggi e il chilometraggio totale e non i dati grezzi utilizzati per ottenere detti punteggi.

112. Occorre inoltre rilevare che laddove i soli dati necessari per l'esecuzione del contratto siano quelli relativi al chilometraggio i dati relativi all'ubicazione non devono essere raccolti.

3.1.1.3 Periodo di conservazione

113. Nel contesto del trattamento di dati effettuato per l'esecuzione di un contratto (ossia per la prestazione di un servizio) è importante distinguere due tipologie di dati prima di definirne i rispettivi periodi di conservazione:

- **dati commerciali e dati relativi alle operazioni:** questi dati possono essere conservati in una banca dati attiva per l'intera durata del contratto. Al termine del contratto possono essere archiviati fisicamente (su un supporto distinto, ad esempio DVD) o logicamente (tramite gestione delle autorizzazioni) nell'eventualità di un contenzioso. Successivamente, una volta scaduti i termini legali di prescrizione, i dati devono essere cancellati o resi anonimi;

- **dati di utilizzo:** i dati di utilizzo possono essere classificati come dati grezzi o come dati aggregati. Come indicato sopra, laddove possibile, i titolari del trattamento o i responsabili del trattamento non dovrebbero trattare dati grezzi. Se invece il trattamento è necessario, i dati grezzi dovrebbero essere conservati soltanto finché sono necessari all'elaborazione dei dati aggregati e alla verifica della validità del processo di aggregazione. I dati aggregati dovrebbero essere conservati soltanto per il periodo di tempo necessario alla prestazione del servizio o come altrimenti previsto dal diritto dell'Unione o degli Stati membri.

3.1.1.4 Informazione e diritti degli interessati

114. Prima del trattamento di dati personali è necessario fornire all'interessato, in maniera trasparente e comprensibile, le informazioni di cui all'articolo 13 del GDPR. In particolare occorre fornire informazioni riguardanti il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo. In quest'ultimo caso l'EDPB raccomanda di adottare un approccio di tipo esplicativo per evidenziare la differenza tra i dati grezzi e il punteggio ottenuto sulla base di tali dati, sottolineando, se del caso, che l'impresa di assicurazione provvederà a raccogliere unicamente il risultato del punteggio ove appropriato.

115. Laddove i dati siano trattati non all'interno del veicolo ma da parte di un fornitore di servizi telematici per conto del titolare del trattamento (l'impresa di assicurazione), sarebbe utile informare l'interessato che, in questo caso, il fornitore non avrà accesso ai dati direttamente riferiti all'identità del conducente (quali nomi, targhe ecc.). Inoltre, considerata l'importanza di informare gli interessati in merito alle conseguenze del trattamento dei dati personali che li riguardano e dato che gli interessati non dovrebbero essere colti di sorpresa dal trattamento dei loro dati personali, l'EDPB raccomanda di informare l'interessato dell'esistenza della profilazione e delle relative conseguenze anche qualora la profilazione non comporti il processo decisionale automatizzato previsto all'articolo 22 del GDPR.

116. Per quanto riguarda il diritto degli interessati, questi devono essere specificamente informati dei mezzi di cui dispongono per esercitare il diritto di accesso, rettifica, limitazione

e cancellazione. Poiché i dati grezzi raccolti in questo contesto sono forniti dall'interessato (tramite moduli specifici o attraverso la sua attività) e trattati sulla base dell'articolo 6, paragrafo 1, lettera b), del GDPR (esecuzione di un contratto), l'interessato ha la facoltà di esercitare il suo diritto alla portabilità dei dati. Come evidenziato nelle linee guida sul diritto alla portabilità dei dati, l'EDPB raccomanda fortemente ai titolari di "spiegare con chiarezza la differenza fra le categorie di dati che un interessato può ricevere attraverso l'esercizio del diritto alla portabilità anziché del diritto di accesso"[48].

117. Le informazioni possono essere fornite all'atto della sottoscrizione del contratto.

3.1.1.5 Destinatario

118. L'EDPB raccomanda che, nei limiti del possibile, i dati relativi all'utilizzo del veicolo siano trattati direttamente all'interno delle *telematic box*, affinché l'assicuratore abbia accesso unicamente ai dati dei risultati (ad esempio un punteggio) e non ai dati grezzi dettagliati.

119. Qualora i dati siano raccolti da un fornitore di servizi telematici per conto del titolare del trattamento (l'impresa di assicurazione) per generare punteggi numerici, il fornitore non avrà bisogno di conoscere l'identità del conducente (ad esempio nomi, targhe ecc.) o dei contraenti.

3.1.1.6 Sicurezza

120. Valgono le raccomandazioni generali. Cfr. la sezione 2.7.

3.1.2 Affitto e prenotazione di un posto auto

121. Il proprietario di un posto auto decide di affittarlo. A tale scopo inserisce un annuncio e fissa il prezzo del posto auto su un'applicazione web. A inserimento effettuato, l'applicazione avvisa il proprietario ogni qual volta un conducente desideri prenotare il posto auto. Il conducente può scegliere una destinazione e verificare la disponibilità di parcheggi sulla base di una molteplicità di criteri. Ottenuta l'approvazione del proprietario, l'operazione è confermata e il fornitore del servizio tratta il pagamento e poi utilizza la navigazione per guidare l'utente fino a destinazione.

3.1.2.1 Base giuridica

122. Quando i dati sono raccolti per mezzo di una comunicazione elettronica accessibile al pubblico si applica l'articolo 5, paragrafo 3, della direttiva e-privacy.

123. Trattandosi di un servizio della società dell'informazione, l'articolo 5, paragrafo 3, della direttiva e-privacy non richiede l'ottenimento del consenso per poter accedere alle informazioni già archiviate nel veicolo qualora tale servizio sia esplicitamente richiesto dall'abbonato.

124. Per il trattamento di dati personali ed esclusivamente per i dati necessari all'esecuzione del contratto di cui l'interessato è parte la base giuridica sarà costituita dall'articolo 6, paragrafo 1, lettera b), del GDPR.

3.1.2.2 Dati raccolti

125. I dati trattati comprendono i dati di contatto del conducente (nome, e-mail, recapito telefonico), il tipo di veicolo (ad esempio autovettura, autocarro, motociclo), il numero di targa, il periodo di sosta, gli estremi del pagamento (ad esempio dati della carta di credito) nonché i dati di navigazione.

[48] Gruppo di lavoro Articolo 29, Linee-guida sul diritto alla "portabilità dei dati" (WP242) rev.01, approvate dall'EDPB, pag. 13.

3.1.2.3 *Periodo di conservazione*

126. I dati dovrebbero essere conservati finché sono necessari all'esecuzione del contratto di parcheggio o come altrimenti previsto dal diritto dell'Unione o degli Stati membri. Al termine di tale periodo i dati sono cancellati o resi anonimi.

3.1.2.4 *Informazione e diritti degli interessati*

127. Prima del trattamento di dati personali si dovrebbero fornire all'interessato, in maniera trasparente e comprensibile, le informazioni di cui all'articolo 13 del GDPR.

128. L'interessato dovrebbe essere specificamente informato dei mezzi di cui dispone per esercitare il diritto di accesso, rettifica, limitazione e cancellazione. Poiché i dati raccolti in questo contesto sono forniti dall'interessato (tramite moduli specifici o attraverso la sua attività) e trattati sulla base dell'articolo 6, paragrafo 1, lettera b), del GDPR (esecuzione di un contratto), l'interessato ha la facoltà di esercitare il suo diritto alla portabilità dei dati. Come evidenziato nelle linee guida sul diritto alla portabilità dei dati, l'EDPB raccomanda vivamente ai titolari di "*spiegare con chiarezza la differenza fra le categorie di dati che un interessato può ricevere attraverso l'esercizio del diritto alla portabilità anziché del diritto di accesso*".

3.1.2.5 Destinatario

129. In linea di massima soltanto il titolare del trattamento e il responsabile del trattamento hanno accesso ai dati.

3.1.2.6 *Sicurezza*

130. Valgono le raccomandazioni generali. Cfr. la sezione 2.7.

3.2 eCall

131. In caso di incidente grave nell'Unione europea, il veicolo attiva automaticamente una chiamata eCall al numero 112, il numero di emergenza valido per tutta l'UE (per maggiori dettagli, cfr. la sezione 1.1) che consente l'invio tempestivo di un'ambulanza nel luogo dell'incidente a norma del regolamento (UE) 2015/758, del 29 aprile 2015, relativo ai requisiti di omologazione per lo sviluppo del sistema eCall di bordo basato sul servizio 112 e che modifica la direttiva 2007/46/CE (di seguito "regolamento (UE) 2015/758").

132. In effetti il generatore eCall installato all'interno del veicolo, che consente la trasmissione tramite una rete mobile di comunicazione senza fili, avvia una chiamata di emergenza, che è attivata automaticamente da sensori di bordo o manualmente dagli occupanti del veicolo soltanto in caso di incidente. Oltre all'attivazione del canale audio, il secondo evento attivato in automatico a seguito di un incidente consiste nel generare la serie minima di dati (Minimum Set of Data - MSD) e nel trasmetterla al centro di raccolta delle chiamate di emergenza (PSAP).

3.2.1 Base giuridica

133. Per quanto riguarda l'applicazione della direttiva e-privacy, occorre prendere in considerazione due disposizioni:

- l'articolo 9 riguardante i dati relativi all'ubicazione diversi dai dati relativi al traffico, che si applica soltanto ai servizi di comunicazione elettronica;
- l'articolo 5, paragrafo 3, per l'accesso alle informazioni archiviate nel generatore installato all'interno del veicolo.

134. Sebbene, in linea di massima, dette disposizioni prevedano il consenso dell'interessato, il regolamento (UE) 2015/758 costituisce un obbligo legale a cui il titolare del trattamento è soggetto (l'interessato non è in grado di operare una scelta autenticamente libera e sarà nell'impossibilità di rifiutare il trattamento dei dati che lo riguardano). Pertanto il

regolamento (UE) 2015/758 prevale sulla necessità di ottenere il consenso del conducente per il trattamento dei dati relativi all'ubicazione e dell'MSD[49].

135. La base giuridica del trattamento di tali dati sarà l'adempimento di un obbligo legale come previsto dall'articolo 6, paragrafo 1, lettera c), del GDPR (ossia il regolamento (UE) 2015/758).

3.2.2 Dati raccolti

136. Il regolamento (UE) 2015/758 stabilisce che i dati inviati dal sistema eCall di bordo basato sul 112 contengono solo le informazioni minime di cui alla norma EN 15722:2015 "Sistemi intelligenti di trasporto — eSafety — serie minima di dati per chiamate eCall (MSD)", ossia:

- l'indicazione dell'attivazione manuale o automatica della chiamata eCall;
- il tipo di veicolo;
- il numero di identificazione del veicolo (VIN);
- il tipo di propulsione del veicolo;
- la marcatura temporale del messaggio di dati iniziale generato nell'ambito dell'evento eCall in corso;
- le ultime coordinate di latitudine e longitudine note del veicolo, determinate il più tardi possibile prima che sia generato il messaggio;
- l'ultima direzione di marcia reale nota del veicolo, determinata il più tardi possibile prima che sia generato il messaggio (soltanto le ultime tre posizioni del veicolo).

3.2.3 Periodo di conservazione

137. Il regolamento (UE) 2015/758 stabilisce che i dati sono conservati solo per il periodo di tempo necessario ad affrontare le situazioni di emergenza. Tali dati sono cancellati completamente quando non sono più necessari per tale scopo. Inoltre i dati sono automaticamente e costantemente soppressi dalla memoria interna del sistema eCall. È possibile conservare soltanto le ultime tre posizioni del veicolo per quanto strettamente necessario a indicare la posizione attuale e la direzione di marcia del veicolo al momento dell'evento.

3.2.4 Informazione e diritti degli interessati

138. A norma dell'articolo 6 del regolamento (UE) 2015/758 i costruttori devono fornire informazioni chiare e complete sul trattamento dei dati effettuato attraverso il sistema eCall. Le informazioni sono fornite nel manuale di istruzioni del proprietario separatamente per il sistema eCall di bordo basato sul 112 e i sistemi eCall supportati da servizi di terzi prima dell'utilizzo del sistema. Le informazioni includono:

- il riferimento alla base giuridica per il trattamento;
- la precisazione del fatto che il sistema eCall di bordo basato sul 112 è attivato in automatico;
- le modalità di elaborazione dei dati eseguite dal sistema eCall di bordo basato sul 112;

[49] Occorre rilevare che l'articolo 8, paragrafo 1, lettera f), del mandato negoziale del Consiglio sulla proposta di regolamento "e-privacy" prevede effettivamente una deroga specifica per il sistema eCall in quanto il consenso non è richiesto *se è necessario localizzare l'apparecchiatura terminale quando un utente finale effettua una comunicazione di emergenza al numero unico di emergenza europeo "112" o al numero di emergenza nazionale, in conformità dell'articolo 13, paragrafo 3.*

- le finalità specifiche dell'elaborazione dati di eCall, che è limitata alle situazioni di emergenza di cui all'articolo 5, paragrafo 2, primo comma, del regolamento (UE) 2015/758;
- i tipi di dati raccolti ed elaborati e i destinatari di tali dati;
- il periodo di conservazione dei dati nel sistema eCall di bordo basato sul 112;
- la precisazione del fatto che non vi è alcun controllo costante del veicolo;
- le modalità per l'esercizio dei diritti degli interessati nonché il servizio di contatto responsabile del trattamento delle domande di accesso;
- eventuali informazioni supplementari necessarie riguardo alla tracciabilità, al controllo e al trattamento dei dati personali in relazione alla fornitura di un sistema eCall supportato da servizi di terzi (TPS eCall) e/o di altri servizi a valore aggiunto, che sono soggetti al consenso esplicito del proprietario e conformi al GDPR. Occorre tenere particolarmente conto del fatto che possono esistere differenze tra il trattamento dei dati eseguito mediante il sistema eCall di bordo basato sul 112 e i sistemi TPS eCall di bordo o altri servizi a valore aggiunto.

139. Inoltre anche il fornitore di servizi deve fornire agli interessati, in maniera trasparente e comprensibile, le informazioni di cui all'articolo 13 del GDPR. In particolare l'interessato deve essere informato delle finalità del trattamento cui sono destinati i dati personali, nonché del fatto che il trattamento dei dati personali si basa su un obbligo legale a cui è soggetto il titolare del trattamento.

140. Inoltre, tenendo conto della natura del trattamento, le informazioni sui destinatari o sulle categorie di destinatari dei dati personali dovrebbero essere chiare e gli interessati dovrebbero essere informati del fatto che i dati non sono disponibili al di fuori del sistema eCall di bordo basato sul 112 ad alcuna entità prima dell'attivazione del sistema eCall.

141. Per quanto riguarda i diritti degli interessati, occorre rilevare che, poiché il trattamento è basato su un obbligo legale, il diritto di opposizione e il diritto alla portabilità non si applicano.

3.2.5 Destinatario

142. I dati non sono disponibili al di fuori del sistema eCall di bordo basato sul 112 ad alcuna entità prima dell'attivazione del sistema eCall.

143. Una volta attivato (manualmente dagli occupanti del veicolo o automaticamente non appena un sensore di bordo rileva una collisione grave), il sistema eCall stabilisce una connessione vocale con lo PSAP pertinente e l'MSD è inviato all'operatore dello PSAP.

144. Inoltre i dati trasmessi attraverso il sistema eCall di bordo basato sul 112 e trattati dagli PSAP possono essere trasferiti ai servizi di pronto intervento e ai servizi associati di cui alla decisione n. 585/2014/UE solo in caso di incidenti relativi a eCall e alle condizioni di cui alla stessa decisione e sono utilizzati esclusivamente al fine di conseguire gli obiettivi di tale decisione. I dati trattati dagli PSAP attraverso il sistema eCall di bordo basato sul 112 non sono trasmessi ad alcuna parte terza senza l'esplicito consenso preventivo dell'interessato.

3.2.6 Sicurezza

145. Il regolamento (UE) 2015/758 stabilisce che nel sistema eCall devono essere integrate tecnologie atte a rafforzare la tutela della privacy, al fine di fornire agli utenti un livello di protezione adeguato, nonché le necessarie tutele per prevenire la sorveglianza e gli abusi. Inoltre i costruttori dovrebbero garantire che il sistema eCall basato sul numero 112 e qualunque altro sistema che fornisca un servizio eCall gestito da servizi di terzi o un servizio a valore aggiunto siano progettati in modo tale da non consentire lo scambio di dati personali tra tali sistemi.

146. Per quanto riguarda gli PSAP gli Stati membri dovrebbero assicurarsi che i dati personali siano protetti dagli abusi, compresi la perdita oppure l'accesso e la modifica illegali, e che i protocolli relativi alla conservazione, al periodo di conservazione, al trattamento e alla protezione dei dati personali siano definiti al livello adeguato e debitamente rispettati.

3.3 Studi sull'incidentalità

147. Gli interessati possono partecipare, su base volontaria, a studi sull'incidentalità finalizzati ad approfondire la conoscenza delle cause degli incidenti stradali e, più in generale, a perseguire finalità scientifiche.

3.3.1 Base giuridica

148. Quando i dati sono raccolti attraverso un servizio pubblico di comunicazione elettronica, il titolare del trattamento dovrà ottenere il consenso dell'interessato per poter accedere a informazioni già archiviate nel veicolo come previsto dall'articolo 5, paragrafo 3, della direttiva e-privacy. In questo contesto, infatti, non è applicabile nessuna delle deroghe previste dalle suddette disposizioni: il trattamento non è eseguito al solo fine di effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica né riguarda un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente.

149. Per quanto riguarda il trattamento di dati personali e tenendo conto della varietà e della quantità dei dati personali necessari per gli studi sull'incidentalità, l'EDPB raccomanda che il trattamento sia basato sul consenso preliminare dell'interessato conformemente all'articolo 6 del GDPR. Tale consenso preliminare deve essere espresso in una forma specifica, attraverso la quale l'interessato manifesti la volontà di partecipare allo studio e acconsenta al trattamento dei suoi dati personali per tale finalità. Il consenso deve essere un'espressione di volontà libera, specifica e informata della persona i cui dati sono trattati (ad esempio selezione di una casella non preselezionata o configurazione del computer di bordo per attivare una funzione nel veicolo). Tale consenso deve essere prestato separatamente, per finalità specifiche e non può essere accorpato al contratto di acquisto o leasing di una nuova autovettura; inoltre deve poter essere revocato con la stessa facilità con cui lo si è espresso. La revoca del consenso determina l'interruzione del trattamento e la conseguente cancellazione dei dati dalla banca dati attiva o anonimizzazione degli stessi.

150. Il consenso richiesto a norma dell'articolo 5, paragrafo 3, della direttiva e-privacy e il consenso necessario come fondamento giuridico per il trattamento dei dati possono essere ottenuti nello stesso momento (ad esempio mediante la selezione di una casella che indichi con chiarezza l'oggetto del consenso espresso dall'interessato).

151. Occorre rilevare che, in base alle condizioni del trattamento (natura del titolare del trattamento ecc.), si potrà scegliere legittimamente un'altra base giuridica, purché questa non riduca l'ulteriore tutela offerta dall'articolo 5, paragrafo 3, della direttiva e-privacy (cfr. il punto 15). Qualora il trattamento sia basato su un altro fondamento giuridico come ad esempio l'esecuzione di un compito di interesse pubblico (articolo 6, paragrafo 1, lettera e), del GDPR), l'EDPB raccomanda di includere nello studio gli interessati su base volontaria.

3.3.2 Dati raccolti

152. Il titolare del trattamento raccoglie dati personali strettamente necessari al trattamento.

153. Occorre prendere in considerazione due tipologie di dati:

- **dati relativi ai partecipanti e ai veicoli**;
- **dati tecnici provenienti dai veicoli** (velocità istantanea ecc.).

154. Gli studi scientifici nel campo dell'incidentalità giustificano la raccolta di dati relativi alla velocità istantanea, anche da parte di persone giuridiche che non gestiscono un servizio pubblico in senso stretto.

155. In effetti, come rilevato sopra, l'EDPB ritiene che i dati relativi alla velocità istantanea raccolti nell'ambito di uno studio sull'incidentalità non costituiscano dati relativi a reati per via della destinazione d'uso (ossia non sono raccolti a fini di indagine o perseguimento di un reato), il che ne giustifica la raccolta da parte di persone giuridiche che non gestiscono un servizio pubblico in senso stretto.

3.3.3 Periodo di conservazione

156. È importante distinguere due tipologie di dati. In primo luogo i dati relativi ai partecipanti e ai veicoli possono essere conservati per tutta la durata dello studio. In secondo luogo i dati tecnici provenienti dai veicoli dovrebbero essere conservati per il periodo di tempo più breve possibile per il conseguimento della finalità. A tale proposito cinque anni dalla data di conclusione dello studio rappresentano un periodo di tempo ragionevole. Al termine di tale periodo i dati devono essere cancellati o resi anonimi.

3.3.4 Informazione e diritti degli interessati

157. Prima del trattamento di dati personali è necessario fornire all'interessato, in maniera trasparente e comprensibile, le informazioni di cui all'articolo 13 del GDPR. In particolare in caso di raccolta di dati relativi alla velocità istantanea gli interessati dovrebbero essere specificamente informati della raccolta. Poiché il trattamento di dati è basato sul consenso, l'interessato deve essere specificamente informato dell'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca. Inoltre poiché i dati raccolti in tale contesto sono forniti dall'interessato (tramite moduli specifici o attraverso la sua attività) e trattati sulla base dell'articolo 6, paragrafo 1, lettera a), del GDPR (consenso), l'interessato ha la facoltà di esercitare il suo diritto alla portabilità dei dati. Come evidenziato nelle linee guida sul diritto alla portabilità dei dati, l'EDPB raccomanda vivamente ai titolari di "spiegare con chiarezza la differenza fra le categorie di dati che un interessato può ricevere attraverso l'esercizio del diritto alla portabilità anziché del diritto di accesso". Pertanto il titolare del trattamento dovrebbe offrire una modalità semplice per revocare il consenso, liberamente e in qualsiasi momento, e dovrebbe sviluppare strumenti che gli consentano di rispondere alle richieste di portabilità dei dati.

158. Tali informazioni possono essere fornite al momento della sottoscrizione del modulo con cui l'interessato accetta di partecipare allo studio sull'incidentalità.

3.3.5 Destinatario

159. In linea di massima soltanto il titolare del trattamento e il responsabile del trattamento hanno accesso ai dati.

3.3.6 Sicurezza

160. Come rilevato sopra, le misure di sicurezza poste in essere devono essere adattate al livello di sensibilità dei dati. Se ad esempio lo studio sull'incidentalità comporta la raccolta di dati relativi alla velocità istantanea (o qualunque altro tipo di dati relativi a condanne penali e a reati) l'EDPB raccomanda vivamente di porre in essere misure di sicurezza efficaci, ad esempio:

- attuazione di misure di pseudonimizzazione (ad esempio hashing con chiave segreta di dati quali cognome/nome dell'interessato e numero di serie);
- conservazione dei dati relativi alla velocità istantanea e dei dati relativi all'ubicazione in banche dati separate (ad esempio utilizzando un meccanismo di cifratura all'avanguardia con procedure di approvazione e chiavi distinte);

- e/o cancellazione dei dati relativi all'ubicazione non appena l'evento o la sequenza di riferimento sia qualificato (ad esempio tipo di strada, diurno/notturno) e conservazione dei dati di identificazione diretta in una banca data a se stante a cui abbia accesso soltanto un ristretto numero di persone.

3.4 Furto d'auto

161. In caso di furto gli interessati potrebbero voler tentare di ritrovare il proprio veicolo utilizzando la posizione. L'uso dei dati relativi all'ubicazione è strettamente limitato alle esigenze dell'indagine e alla valutazione del caso da parte delle autorità giudiziarie competenti.

3.4.1 Base giuridica

162. Quando i dati sono raccolti per mezzo di un servizio di comunicazione elettronica accessibile al pubblico si applica l'articolo 5, paragrafo 3, della direttiva e-privacy.

163. Trattandosi di un servizio della società dell'informazione, l'articolo 5, paragrafo 3, della direttiva e-privacy non richiede l'ottenimento del consenso per poter accedere alle informazioni già archiviate nel veicolo qualora tale servizio sia esplicitamente richiesto dall'abbonato.

164. Per quanto riguarda il trattamento di dati personali, il fondamento giuridico per il trattamento dei dati relativi all'ubicazione sarà il consenso del proprietario del veicolo o, se del caso, l'esecuzione di un contratto (soltanto per i dati necessari all'esecuzione del contratto di cui il proprietario del veicolo è parte).

165. Il consenso deve essere un'espressione di volontà libera, specifica e informata della persona i cui dati sono trattati (ad esempio selezione di una casella non preselezionata o configurazione del computer di bordo per attivare una funzione sul veicolo). La libertà di espressione del consenso comporta la possibilità di revocare il consenso in qualsiasi momento e l'interessato dovrebbe esserne espressamente informato. La revoca del consenso determina l'interruzione del trattamento. A questo punto i dati dovrebbero essere cancellati dalla banca dati attiva, resi anonimi oppure archiviati.

3.4.2 Dati raccolti

166. I dati relativi all'ubicazione possono essere trasmessi soltanto a partire dalla denuncia del furto; il resto del tempo non possono essere raccolti su base continuativa.

3.4.3 Periodo di conservazione

167. I dati relativi all'ubicazione possono essere conservati esclusivamente per il periodo durante il quale il caso è oggetto di valutazione da parte delle autorità giudiziarie competenti, oppure fino al termine di una procedura di accertamento che non si concluda con la conferma del furto del veicolo.

3.4.4 Informazione dell'interessato

168. Prima del trattamento di dati personali si dovrebbero fornire all'interessato, in maniera trasparente e comprensibile, le informazioni di cui all'articolo 13 del GDPR. Più specificamente l'EDPB raccomanda che il titolare del trattamento evidenzi che il veicolo non è sottoposto a sorveglianza costante e che i dati relativi all'ubicazione possono essere raccolti e trasmessi soltanto a partire dalla denuncia del furto. Inoltre il titolare del trattamento deve fornire all'interessato informazioni relative al fatto che l'accesso ai dati è consentito soltanto ai funzionari autorizzati della piattaforma di telesorveglianza e alle autorità legalmente autorizzate.

169. Per quanto riguarda i diritti degli interessati, quando il trattamento dei dati è basato sul consenso l'interessato dovrebbe essere specificamente informato dell'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento

basata sul consenso prestato prima della revoca. Inoltre quando i dati raccolti in questo contesto sono forniti dall'interessato (tramite moduli specifici o attraverso la sua attività) e trattati sulla base dell'articolo 6, paragrafo 1, lettera a) (consenso), o dell'articolo 6, paragrafo 1, lettera b) (esecuzione di un contratto), del GDPR l'interessato ha la facoltà di esercitare il suo diritto alla portabilità dei dati. Come evidenziato nelle linee guida sul diritto alla portabilità dei dati, l'EDPB raccomanda vivamente ai titolari di "spiegare con chiarezza la differenza fra le categorie di dati che un interessato può ricevere attraverso l'esercizio del diritto alla portabilità anziché del diritto di accesso".

170. Pertanto il titolare del trattamento dovrebbe offrire una modalità semplice per revocare il consenso (solo laddove il consenso costituisca il fondamento giuridico), liberamente e in qualsiasi momento, e dovrebbe sviluppare strumenti che gli consentano di rispondere alle richieste di portabilità dei dati.

171. Le informazioni possono essere fornite all'atto della sottoscrizione del contratto.

3.4.5 Destinatari

172. Nel caso di una denuncia di furto, i dati relativi all'ubicazione possono essere trasmessi i) ai funzionari autorizzati della piattaforma di telesorveglianza e ii) alle autorità legalmente autorizzate.

3.4.6 Sicurezza

173. Valgono le raccomandazioni generali. Cfr. la sezione 2.7.