Le ultime Linee Guida EDPB sul trattamento dati nel contesto di veicoli e applicazioni connessi alla mobilità: principi di base e prospettive

Author : Sergio Guida

Date : 29 Aprile 2020

L'industria automobilistica ha subito un cambiamento di paradigma verso automobili sempre più connesse e autonome. Le auto intelligenti (*smart cars*) disponibili oggi sono veicoli dotati di sistemi che offrono funzionalità connesse e a valore aggiunto al fine di migliorare l'esperienza-utente (UX) e migliorare la sicurezza delle auto. Entro i prossimi anni, si prevede che **la connettività delle auto intelligenti si espanderà** e le auto intelligenti saranno connesse ad altri veicoli, pedoni e la loro infrastruttura circostante attraverso scambi di informazioni continui (*connected vehicles*), fino ad auto semi-autonome e autonome (ovvero i livelli 4 e 5 di autonomia definiti in SAE J30163), che faranno uso di tecniche avanzate di *Machine Learning* e Intelligenza Artificiale.

Mentre secondo le previsioni ottimistiche i veicoli completamente automatizzati potrebbero essere ampiamente utilizzati entro il 2030, gli esperti scientifici sono più cauti e sottolineano che sono ancora necessarie ulteriori ricerche per costruire un veicolo completamente autonomo, principalmente nei settori dell'IA e della sicurezza informatica. Molto, moltissimo dipenderà anche dai tempi di implementazione generalizzata della **tecnologia 5G**, oggi candidata a diventare il principale standard a livello mondiale per l'*iperconnettività* delle auto.

Nel precedente articolo, relativo proprio allo studio ENISA che definisce le buone pratiche per la sicurezza delle *smart car*, accennavo alle "Linee guida 1/2020 sul trattamento dei dati personali nel contesto dei veicoli connessi e delle applicazioni connesse alla mobilità" che l'EDPB (*European Data Protection Board* – Comitato Europeo per la Protezione dei Dati) ha adottato per pubblica consultazione a fine gennaio 2020.

Entrando nel merito delle Linee Guida, in ogni caso in cui l'elaborazione dei dati nel contesto di veicoli connessi comporti il **trattamento dei dati personali** di individui, il pertinente quadro giuridico dell'UE è il GDPR, Regolamento Generale sulla Protezione dei Dati 2016/679. In aggiunta al GDPR, la direttiva "*ePrivacy*" (2002/58/CE, modificata dalla direttiva 2009/136/CE) stabilisce uno standard specifico per tutti i soggetti che intendano archiviare o accedere alle informazioni archiviate nell'apparecchiatura terminale di un abbonato o utente nello Spazio

economico europeo (SEE).

In effetti, la direttiva *ePrivacy* è una disposizione generale, non si applica solo ai servizi di comunicazione elettronica, ma anche a tutti i soggetti che collocano o leggono informazioni da un'apparecchiatura terminale: il veicolo collegato e tutti i dispositivi a esso collegati devono essere considerati come "apparecchiature terminali" (proprio come un computer, uno *smartphone* o una *smart TV*,) e la direttiva *ePrivacy* deve essere applicata ove pertinente. La definizione precisa parla di a) apparecchiature collegate direttamente o indirettamente all'interfaccia di una rete pubblica di telecomunicazioni per inviare, elaborare o ricevere informazioni oppure b) apparecchiature per stazioni terrestri satellitari.

Come sottolineato dall'EDPB nel suo parere 5/2019 sull'interazione tra la direttiva *ePrivacy* e il GDPR, la direttiva prevede che, di norma, sia richiesto il **consenso preventivo** per la memorizzazione di informazioni o per l'accesso a informazioni già memorizzate nell'apparecchiatura terminale di un abbonato o di un utente. Qualsiasi operazione di trattamento di dati personali a seguito delle suddette operazioni di trattamento deve inoltre avere una base giuridica ai sensi dell'art. 6 GDPR per essere lecita.

Dal momento che il titolare del trattamento dovrà informare l'interessato in merito a tutte le finalità del trattamento, quando si richiede il consenso per la memorizzazione o l'accesso alle informazioni ai sensi dell'art. 5(3) Direttiva *ePrivacy*, il consenso coprirà normalmente anche tali operazioni di trattamento. Il consenso costituirà probabilmente la base giuridica ex GDPR sia per la memorizzazione e l'ottenimento dell'accesso alle informazioni già memorizzate sia per il trattamento dei dati personali a seguito delle suddette operazioni di elaborazione.

L'ambito di applicazione delle Linee Guida si concentra in particolare sul trattamento dei dati personali in relazione all'uso non professionale dei veicoli connessi da parte degli interessati: ad esempio conducenti, passeggeri, proprietari di veicoli, noleggiatori, ecc. Più specificamente, si occupano del dati personali (i) elaborati all'interno del veicolo, (ii) scambiati tra il veicolo e i dispositivi personali a esso collegati (ad es. *smartphone* dell'utente) o (iii) raccolti all'interno del veicolo ed esportati verso entità esterne (ad es. produttori di veicoli, infrastrutture, compagnie assicurative, riparatori di automobili) per ulteriori elaborazioni.

La **definizione del veicolo connesso** deve essere qui intesa come un concetto ampio: può essere definito tale un veicolo dotato di molte centraline elettroniche (ECU) collegate tra loro tramite una rete di bordo (*in-vehicle*) e strutture di connettività che le consentono di condividere informazioni con altri dispositivi sia all'interno che all'esterno del veicolo. Pertanto, i dati possono essere scambiati tra il veicolo e i dispositivi personali ad esso collegati, ad esempio consentendo il *mirroring* delle applicazioni mobili sull'unità *in-dash* dell'auto di informazione e intrattenimento. Inoltre, lo sviluppo di applicazioni mobili autonome, ovvero indipendenti dal veicolo (ad esempio, basandosi sull'uso esclusivo dello *smartphone*) per aiutare i conducenti, è incluso nell'ambito di questo documento poiché esse contribuiscono alle capacità di connettività del veicolo.

Le applicazioni per i veicoli connessi sono molteplici e diverse e possono includere:

- *Gestione della mobilità*: funzioni che consentono ai conducenti di raggiungere una destinazione rapidamente e in modo economico, fornendo informazioni tempestive sulla navigazione GPS, condizioni ambientali potenzialmente pericolose (ad esempio strade ghiacciate), congestione del traffico o lavori di costruzione di strade, assistenza per trovare parcheggio o garage, consumo di carburante ottimizzato o tariffe stradali.
- *Gestione del veicolo*: funzioni che dovrebbero aiutare i conducenti a ridurre i costi operativi e migliorare la facilità d'uso, come la notifica delle condizioni del veicolo e i promemoria di servizio, il trasferimento dei dati di utilizzo (ad esempio, per i servizi di riparazione del veicolo), assicurazione personalizzata tipo "Paghi come guidi", operazioni a distanza (ad es. Sistema di riscaldamento) o configurazioni del profilo (ad es. posizione del sedile).
- *Sicurezza stradale*: funzioni che avvisano il conducente di pericoli esterni e risposte interne, come protezione da collisioni, avvisi di pericolo, avvisi di abbandono di corsia, rilevamento di sonnolenza del conducente, chiamata di emergenza (*eCall*) o "scatole nere" (registratori di dati/modalità di guida).
- *Intrattenimento*: funzioni che forniscono informazioni e implicano l'intrattenimento di guidatore e passeggeri, come interfacce per *smartphone* (chiamate in vivavoce, messaggi di testo generati dalla voce), *hot spot WLAN*, musica, video, Internet, *social media*.
- *Assistenza alla guida*: funzioni che implicano la guida parzialmente o completamente automatizzata, come l'assistenza operativa o il pilota automatico in situazioni di traffico intenso, parcheggi o autostrade.
- *Benessere*: funzioni che monitorano il comfort, la capacità e l'idoneità del guidatore a guidare come il rilevamento della fatica o l'assistenza medica.

I veicoli possono essere collegati in modo nativo o meno e i dati personali possono essere raccolti attraverso diversi mezzi, tra cui: (i) sensori del veicolo, (ii) box telematici o (iii) applicazioni mobili (ad esempio accessibili da un dispositivo appartenente al conducente). Per rientrare nell'ambito di questo documento, le **applicazioni mobili** devono essere correlate all'ambiente di guida. Ad esempio, le applicazioni di navigazione GPS rientrano assolutamente nell'ambito di applicazione, mentre le applicazioni che suggeriscono all'utente luoghi di suo interesse (ristoranti, monumenti storici, ecc.) non saranno coperte da questo documento.

Gran parte dei dati generati da un veicolo connesso si riferiscono a una persona fisica identificata o identificabile e pertanto costituiscono dati personali. I dati includono dati identificabili **direttamente** (ad esempio, l'identità completa del conducente), nonché dati identificabili **indirettamente** come i dettagli dei viaggi effettuati, i dati di utilizzo del veicolo (ad esempio, i dati relativi allo stile di guida o alla distanza percorsa), oppure i dati tecnici del veicolo (ad es. dati relativi all'usura delle parti del veicolo) che, facendo riferimento a altri file e in particolare al numero di identificazione del veicolo (*VIN*), possono essere correlati a una persona fisica. I dati personali nei veicoli connessi possono anche includere metadati, come lo stato di manutenzione del veicolo.

Alcuni dati generati da veicoli connessi possono anche meritare un'attenzione particolare, data la loro “sensibilità” e/o potenziale impatto sui diritti degli interessati. Allo stato attuale, l'EDPB ha identificato tre categorie di dati personali che meritano particolare attenzione da parte dei

produttori di veicoli e attrezzature, fornitori di servizi e altri titolari del trattamento dei dati (e specifiche prescrizioni): dati sulla posizione, dati biometrici (e qualsiasi categoria speciale di dati come definita nell'articolo 9 GDPR) e dati che potrebbero rivelare reati o violazioni del traffico.

In altre parole, tutti i dati che possono essere associati a una persona fisica rientrano pertanto nell'ambito di queste Linee Guida.

Tenendo conto del volume e della diversità dei dati personali prodotti dai veicoli connessi veicoli connessi, l'EDPB rileva che i titolari del trattamento dei dati sono tenuti a garantire che le tecnologie impiegate nel contesto dei veicoli connessi siano configurate per rispettare la privacy delle persone applicando gli obblighi di protezione dei dati *by design and by default* come richiesto dall'art. 25 GDPR. Le tecnologie dovrebbero essere progettate per **ridurre al minimo la raccolta di dati personali**, fornire impostazioni predefinite di protezione della privacy e garantire che gli interessati siano ben informati e abbiano la possibilità di modificare facilmente le configurazioni associate ai loro dati personali.

Una guida specifica su come i produttori e i fornitori di servizi possano conformarsi alla protezione dei dati *by design and by default* potrebbe essere vantaggiosa per il settore. Alcune pratiche generali, descritte di seguito, possono già contribuire a mitigare i rischi per i diritti e le libertà delle persone fisiche associate ai veicoli connessi.

In generale, i produttori di veicoli e attrezzature, i fornitori di servizi e altri titolari del trattamento dei dati dovrebbero, ove possibile, utilizzare processi che non comportino dati personali o il trasferimento di dati personali al di fuori del veicolo (vale a dire, i dati vengano elaborati internamente).

Questo scenario offre il vantaggio di garantire all'utente il controllo esclusivo e completo dei propri dati personali e, in quanto tale, presenta - “*by design*” - **minori rischi per la privacy**, in particolare vietando qualsiasi trattamento di dati da parte delle parti interessate all'insaputa dell'interessato. Consente inoltre il trattamento di dati particolari (‘sensibili’) come dati biometrici o relativi a reati o altre infrazioni, nonché dati dettagliati sulla posizione che altrimenti sarebbero soggetti a regole più rigorose. Allo stesso modo, presenta meno rischi per la *cybersecurity* e comporta poca latenza (ecco che torna la rilevanza del 5G!), il che lo rende particolarmente adatto alle funzioni di assistenza alla guida automatica.

L'elaborazione locale dei dati (*in car*) dovrebbe essere presa in considerazione dalle case automobilistiche e dai fornitori di servizi ogni qualvolta possibile per mitigare i potenziali rischi dell'elaborazione *in cloud*, come sottolineato nel parere sul *cloud computing* rilasciato dal gruppo di lavoro Articolo 29 (Article 29 Working Party, ora EDPB).

Questo, da un lato, migliorerà lo sviluppo di servizi incentrati sull'utente e, dall'altro, faciliterà e garantirà in futuro ulteriori usi che potrebbero rientrare nell'ambito del GDPR. Più specificamente, l'EDPB raccomanda di sviluppare una piattaforma applicativa *in-car* sicura, divisa fisicamente dalle funzioni della macchina rilevanti per la sicurezza, in modo che l'accesso ai dati delle auto non dipenda da funzionalità *cloud* esterne non necessarie.

In generale, gli utenti dovrebbero essere in grado di controllare il modo in cui i loro dati vengono raccolti ed elaborati nel veicolo:

- le informazioni relative al trattamento devono essere fornite nella lingua del conducente (manuale, impostazioni, ecc.);
- l'EDPB raccomanda che vengano trattati *di default* solo i dati strettamente necessari per il funzionamento del veicolo. Gli interessati dovrebbero avere la possibilità di attivare o disattivare il trattamento dei dati per ogni altro scopo e titolare/responsabile del trattamento e avere la possibilità di eliminare i dati in questione;
- i dati non devono essere trasmessi a terzi (ovvero, l'utente ha accesso esclusivo ai dati);
- i dati devono essere conservati solo per il tempo necessario alla fornitura del servizio o altrimenti richiesto dalla normativa dell'Unione o degli Stati membri;
- gli interessati dovrebbero essere in grado di eliminare definitivamente tutti i dati personali prima che i veicoli siano messi in vendita;
- ove possibile, gli interessati dovrebbero avere accesso diretto ai dati generati da tali applicazioni.

Infine, sebbene possa non essere sempre possibile ricorrere all'elaborazione dei dati locali per ogni caso d'uso, è spesso possibile mettere in atto un **"trattamento ibrido"**. Ad esempio, nel contesto dell'assicurazione basata sull'utilizzo, i dati personali relativi al comportamento alla guida (come la forza esercitata sul pedale del freno, il chilometraggio, ecc.) potrebbero essere elaborati all'interno del veicolo o dal fornitore di servizi telematici per conto della compagnia di assicurazione (il titolare del trattamento dei dati) per generare punteggi numerici che vengono trasferiti alla compagnia di assicurazione su una base definita (ad esempio base mensile). In questo modo, la compagnia assicurativa non ottiene l'accesso ai dati comportamentali grezzi ma solo al punteggio aggregato che è il risultato del trattamento. Ciò garantisce che i principi di minimizzazione dei dati siano soddisfatti *by design*. Ciò significa anche che gli utenti devono avere la possibilità di esercitare i propri diritti quando i dati sono archiviati da altre parti: ad esempio, un utente dovrebbe avere la possibilità di eliminare i dati memorizzati nei sistemi di un'officina di manutenzione o di una concessionaria.

Se proprio i dati devono lasciare il veicolo, è necessario considerare la possibilità di **anonimizzarli** prima di essere trasmessi. L'EDPB ricorda che i principi di protezione dei dati non si applicano alle informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o ai dati personali resi anonimi in modo tale che l'interessato non sia o non sia più identificabile. Una volta che un set di dati è veramente anonimo e le persone non sono più identificabili, la legge europea sulla protezione dei dati non si applica più. Di conseguenza, l'anonimizzazione, ove pertinente, può essere una buona strategia per mantenere i benefici e mitigare i rischi in relazione ai veicoli connessi.

I costruttori di veicoli e apparecchiature, i fornitori di servizi e altri titolari del trattamento dei dati devono, poi, adottare misure che garantiscano la sicurezza e la riservatezza dei dati trattati e tutte le **precauzioni necessarie**. In particolare, va considerata l'adozione delle seguenti misure:

- crittografia dei canali di comunicazione mediante un algoritmo all'avanguardia;
- mettere in atto un sistema di gestione delle chiavi di crittografia unico per ciascun

veicolo, non per ciascun modello;
- se archiviati in remoto, crittografando i dati mediante algoritmi all'avanguardia;
- rinnovare regolarmente le chiavi di crittografia;
- proteggere le chiavi di crittografia da qualsiasi divulgazione;
- autenticazione dei dispositivi di ricezione dei dati;
- assicurare l'integrità dei dati (ad es. tramite *hashing*);
- subordinare l'accesso ai dati personali a tecniche di autenticazione dell'utente affidabili (password, certificato elettronico, ecc.).

Infine, queste raccomandazioni generali devono essere completate da requisiti specifici che tengano conto delle caratteristiche e delle finalità di ciascun trattamento di dati.

Articolo a cura di **Sergio Guida**