42 BRIEF n. 02

Veicoli connessi, controllo non autonomo

Il veicolo connesso raccoglie immagini, suoni e posizioni e resta raggiungibile dal costruttore per tutta la sua vita. Il diritto europeo lo divide in tre discipline, e nessuna lo governa come tale.

Giuseppe Vaciago, Partner, 42 Law Firm[1]
Matteo Flora, Founder & CEO, The Fool

Key Points

1. Ogni veicolo connesso porta a bordo telecamere, microfoni, un sistema di localizzazione e una SIM che il costruttore raggiunge a distanza per tutta la vita del mezzo. Le prove condotte in Norvegia e in Australia mostrano che quel canale permette di vedere, di ascoltare e, nel caso di un autobus, di fermare il veicolo.
2. Il canale serve alla manutenzione e alla sicurezza, ma allo stato nessuna norma europea stabilisce in modo specifico chi possa usarlo, da dove e con quali limiti, perché le regole vigenti si occupano del veicolo, dei sistemi dell'azienda e dei dati, lasciando scoperto proprio il collegamento tra loro.
3. L'Italia ha già scritto la regola che serve quando, nel 2026, ha imposto che i dati raccolti dagli pneumatici intelligenti di Pirelli restassero in Europa: si tratta di estenderla alle auto di servizio, alle flotte di polizia e agli autobus, con un criterio valido per ogni costruttore e prima delle prossime gare.

Executive Summary

Questo brief propone al Governo, all'Agenzia per la cybersicurezza nazionale e alle amministrazioni che acquistano veicoli una regola semplice: chi fornisce un veicolo connesso a una flotta pubblica deve dichiarare chi può raggiungerlo a distanza, da dove e per quali funzioni, e deve mantenere i dati e i servizi informatici che lo governano su infrastrutture soggette al diritto europeo. La regola guarda all'architettura del veicolo e vale per ogni costruttore, poiché il rischio dipende anzitutto dal canale di accesso remoto che ciascun costruttore mantiene sul mezzo e solo in seconda battuta dalla sua nazionalità.

Che il rischio sia concreto lo mostra l'attacco del 28 febbraio 2026 a Teheran, preparato secondo il Financial Times anche osservando la scorta della Guida suprema attraverso le telecamere del traffico, violate da anni[1]; in quell'attacco è stato ucciso Ali Khamenei (sez. I). Un veicolo connesso porta la stessa capacità su ruote, viene parcheggiato ogni giorno davanti a ministeri, basi e abitazioni e resta raggiungibile dal suo costruttore. Il diritto dell'Unione regola il veicolo, i sistemi informatici del costruttore e i dati con tre discipline distinte, nessuna

[1] Le opinioni espresse sono degli autori e non costituiscono parere legale; non riflettono la posizione di clienti dello studio né di enti od organizzazioni presso cui gli autori ricoprono incarichi

delle quali governa quel canale come tale, e la valutazione del rischio adottata dagli Stati membri il 30 gennaio 2026 lo riconosce, pur senza effetti vincolanti.

Le sezioni I-III documentano il problema, la IV spiega perché le norme europee non bastano, la V quali leve italiane esistono già e la VI dettaglia le misure, mentre l'Allegato normativo raccoglie l'analisi giuridica completa e i nodi interpretativi ancora aperti. Il calendario conta, perché le flotte pubbliche si stanno rinnovando ora e un veicolo acquistato senza condizioni sull'accesso remoto resta in servizio per tutta la sua vita utile; le leve per intervenire esistono già nell'ordinamento italiano (l'elenco delle tecnologie strategiche negli acquisti pubblici, il golden power, i capitolati di gara) e la tabella che segue le ordina per destinatario e per tempi, limitandosi alle decisioni pubbliche e ai servizi di cui al par. 6.5 (le indicazioni per le imprese sono al par. 6.4).

Le decisioni in sintesi

Misura	Chi decide	Strumento	Quando
Condurre una valutazione nazionale del rischio sui veicoli connessi e indicare alle amministrazioni i requisiti minimi per auto di servizio e veicoli delle forze di polizia	Agenzia per la cybersicurezza nazionale	Valutazione del rischio e indirizzi alle amministrazioni del perimetro	Subito, in attesa del decreto
Inserire veicoli connessi, moduli telematici e relativi servizi informatici tra le tecnologie strategiche degli acquisti pubblici	Presidenza del Consiglio, con l'Agenzia per la cybersicurezza nazionale	Aggiornamento del decreto del Presidente del Consiglio dei ministri (DPCM) del 30 aprile 2025, come già avvenuto per il 4G e il 5G	Subito: basta un decreto
Chiedere nelle gare la dichiarazione dei flussi di dati, dati e servizi su infrastrutture europee, la telemetria disattivabile, gli aggiornamenti approvati dall'operatore, una prova di isolamento e le SIM sotto il controllo dell'operatore (per i veicoli a guida automatizzata, accesso governato: par. 6.2)	Amministrazioni, forze di polizia, aziende di trasporto pubblico locale	Capitolato di gara	Dalla prossima gara, senza attendere nuove norme
Ammettere nei siti sensibili solo veicoli con sensori disattivati, parcheggiati all'esterno o con sospensione automatica della registrazione nell'area, e vietare di collegare i telefoni di servizio ai sistemi di bordo	Amministrazioni responsabili dei siti, su indirizzo dell'Agenzia	Regole di accesso ai siti	Subito
Applicare a stabilimenti e joint venture di costruttori di veicoli connessi le condizioni sui dati del precedente Pirelli	Presidenza del Consiglio	Prescrizioni del golden power	Alla prossima operazione notificata
Estendere ai costruttori l'obbligo di notificare entro 24 ore le vulnerabilità sfruttate e la tutela contro l'accesso di governi di Paesi terzi, e considerare nell'omologazione il costruttore soggetto a un ordinamento che può imporgli di collaborare	Governo, in sede di Consiglio dell'Unione	Revisione di Cyber Resilience Act, Regolamento ONU n. 155 e Data Act	Alla prima finestra di revisione

Misura	Chi decide	Strumento	Quando
Mettere le immagini delle flotte a servizio di amministrazioni e gestori di reti solo con anonimizzazione verificata e dati in Europa, e con una convenzione per le segnalazioni alla polizia locale	Operatori di flotte e amministrazioni destinatarie	Progettazione del servizio, valutazione d'impatto, convenzione	Prima dell'avvio del servizio

I. Teheran: la telecamera che inquadrava il parcheggio

Secondo il Financial Times, la cui ricostruzione è stata confermata in modo indipendente dall'Associated Press il 23 marzo 2026, le immagini delle telecamere del traffico di Teheran venivano cifrate e trasmesse da anni a server in Israele[1]. Una telecamera in particolare inquadrava l'area vicina a via Pasteur in cui autisti e guardie del corpo degli alti funzionari lasciavano le auto private, e algoritmi complessi aggiungevano dettagli a un dossier per ciascun membro della scorta: indirizzo, orari di servizio, percorso casa-lavoro e, soprattutto, la persona che ciascuno era incaricato di proteggere. In gergo d'intelligence si chiama «pattern of life», ossia il profilo delle abitudini di una persona ricostruito dai suoi spostamenti.

Un dettaglio cambia tutto: la telecamera decisiva inquadrava un parcheggio. A rendere prevedibile la leadership sono state le auto e le abitudini di chi la proteggeva, osservate da un'infrastruttura che nessuno considerava sensibile, tanto che nel novembre 2025 il responsabile della società che gestisce il controllo del traffico di Teheran aveva escluso che quelle telecamere fossero collegate a internet[2].

Fin qui la cronaca. La domanda, per un giurista, è un'altra: che cosa accade quando la telecamera non è più fissata a un palo, ma montata su un veicolo che viene parcheggiato davanti ai luoghi sensibili e che il suo costruttore può interrogare a distanza?

II. Il veicolo come sensore: che cosa vede, che cosa sente, chi lo comanda

Le verifiche tecniche condotte tra il 2025 e il 2026 rispondono su tre piani, in ordine di gravità crescente.

Il primo riguarda ciò che il veicolo vede. A gennaio 2026 Telenor e l'Università della Norvegia sud-orientale hanno presentato i risultati del progetto Lion Cage, secondo i quali, su un SUV elettrico NIO ES8 dotato di sette telecamere, circa il 90 per cento dei pacchetti di rete misurati era diretto verso la Cina e il 70 per cento viaggiava cifrato con un protocollo non documentato[3]. Il 21 settembre 2026 l'inchiesta Asleep at the Wheel della televisione pubblica australiana ABC ha documentato che alcune telecamere della Leapmotor C10 sono prodotte da Dahua, lo stesso fornitore le cui telecamere il governo australiano aveva rimosso dagli edifici federali nel 2023[4]; Stellantis Australia, che distribuisce il marchio, ha replicato che quelle telecamere non registrano e non trasmettono immagini a terzi.

Il secondo riguarda ciò che il veicolo sente. Nella stessa inchiesta i ricercatori di Fortify Labs hanno acceso il microfono di bordo di un pick-up BYD Shark 6 e registrato una telefonata, seguendo nel frattempo in tempo reale la posizione del mezzo[5]. L'accesso iniziale era fisico, e i

ricercatori lo hanno presentato come simulazione dell'accesso di cui il costruttore dispone sui propri veicoli; il costruttore ha riconosciuto l'esistenza di un difetto del software. Sul piano istituzionale, il 28 maggio 2026 la vicedirettrice generale dell'intelligence australiana, Lisa Alonso Love, ha raccomandato ai parlamentari di non tenere conversazioni riservate in alcun veicolo, connesso o meno, osservando che un'auto connessa «può avere altri vettori per raccogliere quelle informazioni»[6].

Il terzo piano, il più grave, riguarda chi comanda il veicolo. Nel 2025 l'azienda di trasporto pubblico di Oslo, Ruter, ha messo alla prova due autobus elettrici in una miniera, al riparo dalle reti, e ha verificato che sul modello cinese del 2025 il costruttore poteva raggiungere da remoto le funzioni critiche fino a fermare il mezzo, mentre sul modello europeo del 2022 questo non era possibile[7]. L'inchiesta ABC ha mostrato inoltre un dipendente di XPeng, intervistato in forma anonima, che senza alcuna violazione osservava in tempo reale posizione, velocità, angolo di sterzo e sedile del passeggero di un'auto in marcia a Sydney, insieme a un registro di aggiornamenti installati a distanza, alcuni dei quali senza il consenso esplicito dei proprietari[4].

Nel caso BYD i ricercatori hanno simulato l'accesso di cui dispone il costruttore; negli altri casi non è servito alcun attacco, perché il canale fa parte del progetto del veicolo e serve alla diagnosi, alla telemetria imposta dall'omologazione, agli aggiornamenti del software e, nei veicoli a guida automatizzata, all'intervento a distanza, che il diritto europeo contempla espressamente per i veicoli completamente automatizzati[8]. È come se ogni auto di servizio custodisse un badge che apre tutte le porte dell'ufficio, valido per l'intera vita del mezzo e intestato a un soggetto che l'amministrazione non conosce: il badge serve, e il problema nasce dal fatto che nessuno sappia chi lo usa, quando e da dove.

> **Executive Takeaway. Il veicolo connesso vede e sente, e un autobus in prova a Oslo poteva essere fermato a distanza dal costruttore: sono funzioni previste dal progetto, e il rischio dipende da chi le governa.**

III. La bandiera e la porta

Il primo equivoco da sciogliere è questo. La fiducia geopolitica guarda alla provenienza del costruttore; la sicurezza del veicolo guarda all'accesso. Le due nozioni si sovrappongono solo in parte, poiché un costruttore europeo che mantiene un canale di accesso remoto non governato espone il veicolo quanto un costruttore extraeuropeo, mentre un veicolo di qualunque provenienza le cui funzioni critiche siano isolate dalla rete lo espone assai meno. La stessa presentazione di Lion Cage conclude che il rischio dipende dall'architettura e dal modello di business, e che la documentazione e le dichiarazioni dei costruttori non sono affidabili[3].

La logica dell'accesso è anche il criterio per costruire bene i servizi che usano i dati del veicolo per scopi di interesse pubblico. Chi gestisce una flotta di veicoli connessi può mettere le immagini raccolte durante il servizio a disposizione della polizia locale, per segnalare possibili violazioni del codice della strada, oppure dei gestori delle reti di luce e gas, per individuare pali pericolanti e guasti visibili dalla strada; sono servizi utili alla collettività, e il loro esito dipende ancora una volta da come è governato il canale (chi riceve le immagini, per quale finalità, dopo

quale trattamento e su quale base giuridica). Per le segnalazioni puntuali la via è praticabile già oggi, mentre i flussi sistematici richiedono una convenzione con l'amministrazione e, in prospettiva, una norma di legge (par. 6.5); l'accertamento resta comunque riservato agli organi di polizia stradale, per i quali le immagini dell'operatore costituiscono una segnalazione da cui muovere[9].

I Paesi che hanno già reagito si collocano lungo la distinzione tra provenienza e accesso. Gli Stati Uniti hanno scelto il criterio della provenienza: la regola definitiva del Bureau of Industry and Security del 14 gennaio 2025 vieta il software di origine cinese o russa a partire dai modelli 2027 e l'hardware dai modelli 2030[10]. La Polonia ha combinato i due criteri, perché l'ordine del Capo di Stato maggiore annunciato il 17 febbraio 2026 vieta l'ingresso nelle installazioni militari protette ai veicoli prodotti in Cina, ammette gli altri veicoli dotati di dispositivi che registrano posizione, immagine o suono solo a funzioni disattivate e chiede al Governo un'omologazione «in materia di sicurezza delle informazioni» fondata su meccanismi «trasparenti e non discriminatori»[11]. L'Australia procede caso per caso, con raccomandazioni e parcheggi lontani dai siti sensibili, senza aver ancora fissato standard per i veicoli[4], mentre l'Unione europea dispone di un'analisi e non ancora di una regola[12].

L'obiezione va presa nella sua versione più forte: una regola sui veicoli connessi rischia di diventare protezionismo industriale presentato come sicurezza. C'è del vero, e va riconosciuto, perché i ricercatori di Fortify Labs avvertono che il problema riguarda anche i costruttori non cinesi, l'intelligence australiana non ha nominato marche né Paesi e il NIS Cooperation Group (il gruppo di cooperazione tra gli Stati membri previsto dalla direttiva NIS2) ragiona di architetture e di fornitori sottoposti a pressioni governative senza indicare nazionalità. Sarebbe però sbagliato concluderne che non serve alcuna regola. Proprio perché il canale esiste in ogni veicolo connesso, la regola deve guardare all'architettura e valere per tutti i costruttori, e la provenienza vi entra come fattore di rischio non tecnico, ossia come soggezione del costruttore a un ordinamento che può imporgli di collaborare con i propri apparati di sicurezza. È anche la forma che regge meglio al vaglio della non discriminazione, come riconosce la stessa richiesta polacca.

IV. Il diritto che divide il veicolo in tre

Il diritto dell'Unione scompone il veicolo connesso in tre oggetti: il veicolo è disciplinato dall'omologazione, i sistemi informatici da cui il costruttore gestisce telemetria e aggiornamenti (il cosiddetto backend) ricadono nella direttiva sulla sicurezza delle reti e dei sistemi informativi (NIS2) come sistemi dell'impresa, i dati sono regolati dal Data Act e dal regolamento generale sulla protezione dei dati (GDPR). Ciascuna disciplina regola un pezzo, mentre nessuna regola come tale il canale di accesso remoto del costruttore (l'unico spiraglio, offerto dalla NIS2, è discusso nell'Allegato, nodo C.5). Una quarta norma, il Cyber Resilience Act, che impone la notifica rapida delle vulnerabilità, esclude espressamente i veicoli dal proprio ambito. La tabella riassume la scomposizione, che l'Allegato normativo sviluppa norma per norma.

Oggetto	Chi lo regola	Che cosa resta scoperto
Veicolo	Omologazione (Reg. (UE) 2019/2144 e 2018/858, Regolamenti ONU n. 155 e 156)	Il costruttore non è mai considerato una possibile minaccia; la telemetria è obbligatoria, ma nessuna regola dice dove possano andare i dati
Sistemi del costruttore	NIS2 (D.Lgs. 138/2024)	Protegge i sistemi dell'azienda, non la flotta che l'azienda ha venduto
Dati	Data Act e GDPR	Nessun limite su dove il costruttore porti i dati; la tutela contro l'accesso di governi stranieri vale solo per i fornitori di servizi cloud
Vulnerabilità	Cyber Resilience Act	Esclude i veicoli: la notifica entro 24 ore vale per la telecamera da cruscotto venduta separatamente, non per l'auto su cui è montata

Il quadro conferma, quasi alla lettera, la diagnosi del NIS Cooperation Group, la cui valutazione coordinata del 30 gennaio 2026 osserva che un fornitore può usare canali di accesso diretti al veicolo, noti o nascosti, «aggirando di fatto molti dei controlli imposti dalla normativa sull'omologazione», e che quel regime, nato per la sicurezza stradale, «non mitiga a sufficienza tali rischi»[12]: si tratta precisamente dello scenario documentato a Oslo e a Sydney. Il documento chiede agli Stati membri di dotarsi di norme che consentano di limitare o escludere i fornitori ad alto rischio dalle catene di approvvigionamento critiche, ma non è vincolante, e lascia quindi ai singoli Stati la scelta di agire.

> **Executive Takeaway. Il diritto europeo regola il veicolo, il backend e i dati, mentre il canale di accesso remoto del costruttore resta senza una disciplina propria.**

V. Italia: gli attrezzi ci sono, puntati altrove

Allo stato non risultano posizioni pubbliche dell'Agenzia per la cybersicurezza nazionale sui veicoli connessi. L'unico testo istituzionale che lega l'automotive cinese alla sicurezza cibernetica è la relazione del Comitato parlamentare per la sicurezza della Repubblica (COPASIR) trasmessa il 4 agosto 2026, che richiama la «postura di Pechino rispetto al settore delle auto elettriche e dell'automotive in generale, ove il focus è stato posto anche ai profili connessi alla sicurezza fisica e cibernetica», nel contesto degli investimenti e delle joint venture[13].

Lo Stato, tuttavia, la regola l'ha già scritta. Con il decreto del 9 aprile 2026, che riprende e aggiorna quello del 16 giugno 2023, il Governo ha esercitato i poteri speciali su Pirelli a tutela della tecnologia Cyber Tyre, che trasforma lo pneumatico in un sensore capace di raccogliere, tra l'altro, le abitudini degli utenti e le condizioni di guida; le prescrizioni impediscono il trasferimento di beni e servizi informatici e di comunicazione (ICT) verso infrastrutture situate fuori dal territorio in cui si applica il diritto europeo e la condivisione dei dati raccolti con soggetti riconducibili al governo cinese[14]. Il paradosso è servito: l'ordinamento trattiene in Europa i dati raccolti da uno pneumatico italiano, mentre quelli raccolti da un'auto di servizio parcheggiata davanti a un ministero possono finire su server ovunque. Il precedente contiene due criteri distinti, che conviene tenere separati: la localizzazione dei dati e dei servizi informatici guarda all'architettura e vale per chiunque, mentre il divieto di condivisione con un governo determinato guarda alla provenienza. Questo brief propone di estendere il primo.

Resta l'obiezione di chi teme che una regola di questo tipo allontani gli investimenti dei costruttori esteri. Il precedente Pirelli mostra però che le prescrizioni sui dati possono accompagnare un investimento estero senza impedirlo, e una regola sull'architettura, che si applica allo stesso modo a ogni costruttore, espone l'Italia all'accusa di discriminazione molto meno di quanto farebbe un divieto fondato sulla provenienza.

Sarebbe però ingeneroso imputare al golden power il paradosso dello pneumatico, che per sua natura colpisce operazioni societarie su attivi strategici, mentre la vendita di veicoli ne resta fuori. Gli altri attrezzi esistono e si possono aggiornare. Il DPCM del 30 aprile 2025, attuativo dell'art. 14 della legge 90/2024, elenca 22 categorie tecnologiche per le quali le amministrazioni e i soggetti del perimetro di sicurezza nazionale cibernetica devono applicare elementi essenziali di cybersicurezza e criteri di premialità; vi figurano i sistemi di videosorveglianza e il software di controllo dei droni, ma nessuna voce riguarda i veicoli o i moduli telematici[15]. Ne discende che la telecamera fissa acquistata da un ministero è soggetta a quei requisiti, mentre l'auto di servizio con telecamere, microfoni e SIM ne resta esente. Il DPCM 2 ottobre 2025 ha aggiunto all'elenco le reti mobili 4G e 5G, motivando la scelta «nell'attuale contesto geopolitico» a cinque mesi dal primo decreto[15], a riprova del fatto che l'elenco si allarga per decreto quando il contesto lo richiede. La disciplina delle auto di servizio, invece, risale al DPCM 25 settembre 2014 e persegue soltanto obiettivi di risparmio e trasparenza[15].

Nel frattempo le flotte cambiano: Bari ha già aggiudicato, con fondi del Piano nazionale di ripresa e resilienza, la fornitura di 99 autobus elettrici Yutong e Taranto quella di 45 autobus BYD, contratti resi noti all'inizio del 2024[16], senza che, dalle fonti pubbliche consultate, risulti alcuna prova di isolamento paragonabile a quella condotta a Oslo. Il costo dell'inazione si misura proprio qui, perché le condizioni sui dati e sull'accesso remoto si fissano nel capitolato, e per i mezzi già aggiudicati possono ormai soltanto essere rinegoziate con il fornitore.

VI. Implicazioni operative

La risposta non può essere il divieto fondato sulla sola bandiera, né l'attesa di una norma europea che ancora non c'è. Può essere, invece, una regola sull'accesso, che valga per ogni costruttore e che l'ordinamento italiano è già in grado di scrivere con strumenti propri.

6.1 Per il Governo e per l'Agenzia per la cybersicurezza nazionale

Occorre anzitutto una valutazione nazionale del rischio sui veicoli connessi, costruita sul modello di quella del NIS Cooperation Group. Su questa base, quattro interventi si possono costruire su strumenti già esistenti:

1. Aggiornare l'allegato 2 del DPCM 30 aprile 2025 con la categoria «veicoli connessi, moduli telematici e relativi servizi di backend», come già avvenuto per il 4G e il 5G.
2. Regolare l'accesso ai siti sensibili in base all'architettura: veicoli con dispositivi che registrano posizione, immagine o suono ammessi solo a funzioni disattivate o parcheggiati all'esterno, oppure, per i veicoli che non possono circolare a sensori spenti, con garanzie equivalenti come la sospensione automatica della registrazione e della trasmissione nell'area (il cosiddetto geofencing), e divieto di collegare i telefoni di

servizio ai sistemi di bordo per intrattenimento e navigazione (il cosiddetto infotainment).

3. Adottare condizioni standard sui dati nell'esercizio del golden power, ricalcate sulla parte architetturale del precedente Pirelli (localizzazione dei dati e dei servizi ICT nell'Unione, organizzazione di sicurezza dedicata), per stabilimenti e joint venture di costruttori di veicoli connessi, con la provenienza valutata come fattore di rischio aggiuntivo.
4. Indicare alle amministrazioni del perimetro i requisiti minimi per le auto di servizio e per i veicoli delle forze di polizia, in attesa dell'aggiornamento del decreto.

6.2 Per le amministrazioni acquirenti e per le aziende di trasporto pubblico locale

Il capitolato è la leva più rapida, perché non attende alcuna norma. Nelle gare per auto di servizio, flotte e autobus occorre richiedere almeno:

1. La dichiarazione dei flussi di dati e dei loro destinatari, inclusi i soggetti extraeuropei della filiera.
2. La possibilità di disattivare la telemetria non necessaria al funzionamento e alla sicurezza.
3. L'installazione degli aggiornamenti a distanza solo previa approvazione dell'operatore.
4. Una prova di isolamento sul modello di Oslo prima della messa in servizio.
5. Il controllo delle SIM di bordo in capo all'operatore.
6. La localizzazione dei dati del veicolo e dei servizi informatici che lo governano su infrastrutture soggette al diritto europeo.

Per i veicoli a guida automatizzata, nei quali l'intervento a distanza e gli aggiornamenti del software fanno parte del concetto di sicurezza, i requisiti 3, 4 e 5 vanno declinati come accesso governato (dichiarato, tracciato, localizzato nell'Unione e verificabile dall'acquirente), e la prova di isolamento serve allora a verificare che il veicolo sia raggiungibile solo attraverso i canali dichiarati.

6.3 Per il legislatore europeo

Occorre chiudere il varco tra omologazione e Cyber Resilience Act, estendendo ai costruttori di veicoli l'obbligo di notifica entro 24 ore delle vulnerabilità attivamente sfruttate. Occorre inserire nel modello di minaccia del Regolamento ONU n. 155 l'ipotesi che il costruttore sia costretto ad agire da un ordinamento che può imporgli di collaborare con i propri apparati di sicurezza. Occorre, infine, estendere al costruttore, in quanto titolare dei dati del veicolo, la tutela contro l'accesso governativo di Paesi terzi che il Data Act riserva oggi ai fornitori di servizi cloud.

6.4 Per le imprese con flotte aziendali

Per le imprese la conseguenza è concreta: i veicoli connessi della flotta vanno trattati come beni informatici a tutti gli effetti, il che significa inventariarli, adottare regole d'uso coerenti con le raccomandazioni dell'intelligence australiana (nessuna conversazione riservata a bordo,

nessun telefono aziendale collegato all'infotainment) e prevedere clausole sui dati nei contratti con fornitori e società di noleggio. Per i soggetti NIS2 si tratta già di un obbligo, perché la valutazione coordinata sui veicoli connessi è tra quelle di cui devono tenere conto nella scelta dei fornitori.

6.5 Per chi mette a disposizione le immagini delle flotte a fini di utilità pubblica

I servizi che mettono le immagini raccolte dalle flotte a disposizione delle amministrazioni e dei gestori delle reti possono essere progettati in modo conforme fin dall'origine, a condizioni precise che in parte variano secondo il destinatario:

1. Per i servizi ai gestori delle reti, un'anonimizzazione eseguita il prima possibile nella catena del trattamento (a bordo o, quando non è tecnicamente praticabile, in un ambiente separato con accesso ai dati grezzi ristretto e tracciato) e verificata con prove di reidentificazione; per le segnalazioni alla polizia locale, l'oscuramento dei volti e delle altre targhe prima della trasmissione, conservando la sola targa del veicolo in violazione.
2. Il trattamento delle immagini su infrastrutture soggette al diritto europeo, con l'esclusione contrattuale e tecnica dell'accesso ai fotogrammi da parte del costruttore del veicolo, quando diverso dall'operatore del servizio, secondo il criterio dell'accesso governato proposto per le altre flotte.
3. La trasmissione al destinatario dei soli fotogrammi pertinenti all'evento segnalato, in luogo del flusso continuo delle telecamere.
4. La conservazione delle immagini destinate al servizio limitata al tempo necessario alla segnalazione, distinta da quella prevista per le altre finalità dell'operatore.
5. Una valutazione d'impatto sulla protezione dei dati prima dell'avvio, obbligatoria quando il servizio configura una sorveglianza sistematica su larga scala di una zona accessibile al pubblico.
6. Per le segnalazioni alla polizia locale, una convenzione con l'amministrazione che definisca finalità, categorie di violazioni, ruoli delle parti ai fini della protezione dei dati e modalità di verifica da parte dell'organo accertatore, e in prospettiva una norma nazionale che dia a questi flussi una base giuridica certa.

VII. Considerazioni conclusive

A Teheran la telecamera decisiva inquadrava il parcheggio delle auto della scorta; nel veicolo connesso telecamera e parcheggio coincidono, e il canale che li collega al costruttore non ha oggi una norma che lo governi.

Le leve per governarlo esistono già nell'ordinamento italiano ed europeo, e si tratta di puntarle sul veicolo con un criterio fondato sull'architettura e valido per ogni costruttore.

Allegato normativo

L'Allegato raccoglie, per il lettore giurista, l'analisi norma per norma su cui poggiano le sezioni IV-VI e i nodi interpretativi che le misure proposte devono ancora sciogliere.

A. La scomposizione norma per norma

Oggetto	Disciplina	Che cosa impone	Che cosa lascia scoperto
Veicolo	Reg. (UE) 2019/2144 e Reg. ONU n. 155 (cibersicurezza); Reg. (UE) 2018/858 e Reg. ONU n. 156 (aggiornamenti del software)	Sistema di gestione della cibersicurezza certificato per un massimo di tre anni; verifica prevalentemente documentale con prove a campione; monitoraggio dei veicoli in circolazione «attraverso i dati e i log dei veicoli»	Il modello di minaccia considera il backend bersaglio di terzi o di personale infedele, mai il costruttore; la telemetria è obbligatoria ma senza limiti di destinazione; gli esiti del monitoraggio, compresi i nuovi attacchi, si riferiscono all'autorità di omologazione almeno una volta l'anno
Veicolo	Reg. (UE) 2024/2847 (Cyber Resilience Act)	Dall'11 settembre 2026, notifica entro 24 ore delle vulnerabilità attivamente sfruttate	Esclude i prodotti soggetti al Reg. (UE) 2019/2144 (art. 2, par. 2, lett. c): l'obbligo vale per una telecamera da cruscotto venduta separatamente, e non per l'auto
Backend	Dir. (UE) 2022/2555 (NIS2) e D.Lgs. 138/2024	Il costruttore è «soggetto importante» (allegato II, punto 5, lett. e) e protegge i sistemi che «utilizza»	La flotta venduta non è un sistema dell'ente; l'incidente si misura sul servizio, cioè sulla produzione; la giurisdizione segue lo stabilimento (art. 26)
Dati	Reg. (UE) 2023/2854 (Data Act) e GDPR	Accesso dell'utente ai dati; informativa sull'identità del titolare dei dati e delle «altre parti coinvolte» (art. 3, par. 3, lett. d)	Nessun limite di destinazione per il costruttore; la tutela contro l'accesso governativo di Paesi terzi (art. 32) vincola i soli fornitori di servizi cloud
Danno	Dir. (UE) 2024/2853 (prodotti difettosi)	Il fabbricante risponde del software sotto il suo controllo (art. 11, par. 2), anche quando il danno passa per l'azione di un terzo (art. 13)	L'esfiltrazione di dati non è danno risarcibile (art. 6 e considerando 20); beni e dati professionali sono esclusi; si applica ai prodotti immessi dopo il 9 dicembre 2026

Ne discende un'asimmetria di trasparenza che opera già: dall'11 settembre 2026 chi produce una telecamera da cruscotto venduta separatamente deve notificare entro 24 ore una vulnerabilità sfruttata, mentre il costruttore del veicolo su cui è montata ne riferisce all'autorità di omologazione con cadenza almeno annuale[17]. Per gli acquirenti pubblici, la dichiarazione dei flussi di dati richiesta al par. 6.2 può fare leva sull'informativa dell'art. 3, par. 3, lett. d), del Data Act.

B. Le altre discipline e la valutazione del NIS Cooperation Group

Non colmano la lacuna neppure altre due discipline. La direttiva sulle apparecchiature radio (RED, direttiva 2014/53/UE) impone ai moduli radio dei veicoli omologati, dal 1° agosto 2025 e in forza del regolamento delegato (UE) 2022/30, il solo requisito di cibersicurezza relativo alla protezione della rete (art. 3, par. 3, lett. d), esclusi quelli su dati personali e frodi; dall'11 dicembre 2027 anche questo verrà meno (regolamento delegato (UE) 2026/339), per lasciare il campo al Cyber Resilience Act, che però esclude i veicoli. La direttiva sui sistemi di trasporto intelligenti (direttiva 2010/40/UE, modificata dalla direttiva (UE) 2023/2661) e i regolamenti

delegati (UE) n. 886/2013, sulle informazioni minime sulla sicurezza stradale, e (UE) 2022/670, sulle informazioni sul traffico in tempo reale, disciplinano invece la messa a disposizione dei dati sul traffico attraverso i punti di accesso nazionali, non l'accesso del costruttore al veicolo[18].

La valutazione coordinata del NIS Cooperation Group è adottata ai sensi dell'art. 22 della direttiva NIS2; la richiesta agli Stati membri citata nella sez. IV è la raccomandazione R_09. Il documento non è vincolante e produce effetti solo in via indiretta, perché i soggetti NIS2 devono tenerne conto nel valutare i propri fornitori (art. 21, par. 3, della direttiva; art. 24, comma 3, del D.Lgs. 138/2024)[12].

C. Nodi aperti

1. **Libera circolazione dei veicoli omologati.** L'art. 6, par. 5, del Reg. (UE) 2018/858 vieta agli Stati membri di vietare, limitare od ostacolare l'immissione sul mercato, l'immatricolazione o l'entrata in circolazione dei veicoli conformi, salvo i casi previsti dalle clausole di salvaguardia del capo XI[19]. Le misure proposte non incidono su questi momenti, poiché operano sulla scelta d'acquisto delle amministrazioni (decreto e capitolati), sull'accesso a siti determinati e sulle condizioni di un investimento (golden power). Un divieto generale di immatricolazione fondato sul rischio di accesso remoto passerebbe invece per la procedura dell'art. 52, che consente misure restrittive provvisorie quando il veicolo presenta un grave rischio per la salute o la sicurezza delle persone o per altri aspetti di interesse pubblico tutelati dal regolamento; resta da stabilire se la sicurezza delle informazioni rientri tra questi.
2. **Provenienza negli appalti.** Con la sentenza Kolin la Corte di giustizia ha escluso che gli operatori di Paesi terzi privi di un accordo con l'Unione sull'accesso agli appalti possano invocare la parità di trattamento prevista dalle direttive, riconducendo la materia alla competenza esclusiva dell'Unione[20]. Ne discende che un criterio di provenienza adottato da uno Stato membro si muove in un ambito nel quale le misure di portata generale spettano all'Unione. Il criterio architetturale, che vale per tutti gli offerenti, resta pienamente nella disponibilità della stazione appaltante.
3. **Base giuridica dei flussi verso la polizia locale.** Per l'operatore della flotta, la trasmissione delle immagini è un trattamento ulteriore rispetto alla finalità di raccolta, e richiede una norma di legge oppure il superamento del test di compatibilità dell'art. 6, par. 4, del GDPR. Per l'organo che le riceve la disciplina dipende dalla natura dell'illecito, perché le violazioni del codice della strada sono in prevalenza illeciti amministrativi, il cui trattamento ricade nel GDPR, in base all'art. 6, par. 1, lett. e), e non nel D.Lgs. 51/2018, riservato alla prevenzione e al perseguimento dei reati[9]. Resta da stabilire se una convenzione con il Comune basti a sostenere flussi sistematici o se serva la norma nazionale che il par. 6.5 indica in prospettiva.
4. **Accesso remoto e difetto del prodotto.** La direttiva (UE) 2024/2853 include tra le circostanze per valutare il difetto il momento dell'immissione sul mercato oppure, se il fabbricante conserva il controllo del prodotto dopo la vendita, il momento in cui il prodotto esce da quel controllo, e i requisiti di cibersicurezza rilevanti per la sicurezza (art. 7, par. 2, lett. e) e f). Un canale di accesso remoto non governato può quindi rendere

difettoso il veicolo quando ne derivano danni a persone o cose, mentre la sola esfiltrazione di dati resta fuori dal danno risarcibile.

5. **La flotta venduta nella NIS2.** L'art. 21, par. 1, della direttiva NIS2 riferisce le misure di sicurezza ai sistemi che i soggetti utilizzano «nelle loro attività o nella fornitura dei loro servizi». Resta da stabilire se i server da cui il costruttore gestisce telemetria e aggiornamenti della flotta venduta rientrino tra questi, il che porterebbe il canale nell'ambito della direttiva almeno per i costruttori stabiliti nell'Unione.

Note

[1] Mehul Srivastava et al., "Inside the plan to kill Ali Khamenei", Financial Times, 2 marzo 2026, https://www.ft.com/content/bf998c69-ab46-4fa3-aae4-8f18f7387836. Conferma indipendente, con fonti proprie: Dake Kang, Sam Mednick, "Iran built a vast camera network to control dissent. Israel turned it into a targeting tool", Associated Press, 23 marzo 2026, https://www.securityweek.com/iran-built-a-vast-camera-network-to-control-dissent-israel-turned-it-into-a-targeting-tool/. Entrambe le testate riferiscono fonti anonime e non indicano il vettore tecnico della compromissione.

[2] Dichiarazione di Akbar Ekhtiari, responsabile della società di controllo del traffico di Teheran, Entekhab, 16 novembre 2025, https://www.entekhab.ir/fa/news/895258.

[3] Telenor e Università della Norvegia sud-orientale (USN), Lion Cage, presentazione dei risultati, gennaio 2026, https://kollektivtrafikk.no/app/uploads/2026/01/Presentasjon-Lion-Cage.pdf. Le misure sul traffico di rete del veicolo provengono da questa sola fonte e non risultano replicate in modo indipendente.

[4] ABC Four Corners, "Asleep at the Wheel", 21 settembre 2026, https://www.abc.net.au/news/2026-09-21/asleep-at-the-wheel-/107178176; "Australia banned these Chinese CCTV cameras. Now they're turning up in EVs", ABC News, 21 settembre 2026, https://www.abc.net.au/news/2026-09-21/ev-electric-vehicle-leapmotor-chinese-cctv-cameras-dahua-banned/107142310. La replica di Stellantis Australia è riportata da CarsGuide, 25 settembre 2026. Gli episodi relativi a XPeng (osservazione in tempo reale e registro degli aggiornamenti) provengono dalla sola inchiesta ABC; XPeng ha negato di poter immobilizzare a distanza i veicoli venduti in Australia.

[5] "We got a cybersecurity expert to hack this BYD. It was too easy", ABC News, 21 settembre 2026, https://www.abc.net.au/news/2026-09-21/byd-hacked-by-cybersecurity-expert-vehicle-sabotage-surveillance/107139482; per la replica del costruttore e la precisazione di Fortify Labs sull'accesso fisico, CarExpert, 1 ottobre 2026, https://www.carexpert.com.au/car-news/byds-own-shark-6-hacking-investigation-reveals-software-defect.

[6] Senate Legal and Constitutional Affairs Legislation Committee, Budget Estimates, 28 maggio 2026, come riportato da NCA NewsWire, 29 maggio 2026, https://au.news.yahoo.com/sensitive-spy-boss-tells-mps-002548981.html, e da PS News, 5 giugno 2026, https://psnews.com.au/public-servants-warned-to-watch-how-they-talk-shop-in-internet-enhanced-vehicles/179609/. Testo originale: "Obviously, a connected car may have other vectors to gather that information, but those conversations should only ever happen in places that are set up for classified conversations." Il resoconto ufficiale (Hansard, ID 29605) non è stato consultato.

[7] Telenor e USN, Lion Cage, cit.; "Chinese buses in Norway can be remotely controlled", Fortune, 6 novembre 2025, https://fortune.com/2025/11/06/chinese-buses-norway-remote-control.

[8] Regolamento di esecuzione (UE) 2022/1426 della Commissione, del 5 agosto 2022, art. 2, punti 25 e 26, e allegato II, punti 6 e 8, http://publications.europa.eu/resource/celex/32022R1426.

[9] Regolamento (UE) 2016/679 (GDPR), artt. 6, par. 1, lett. e), e par. 4, 25 e 35, par. 3, lett. c), e considerando 50, http://publications.europa.eu/resource/celex/32016R0679; D.Lgs. 30 aprile 1992, n. 285 (codice della strada), art. 12, https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:1992-04-30;285; per il trattamento da parte delle autorità a fini di prevenzione e perseguimento dei reati, D.Lgs. 18 maggio 2018, n. 51, https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2018-05-18;51; Gruppo di lavoro Articolo 29, Parere 05/2014 sulle tecniche di anonimizzazione (WP216), 10 aprile 2014; European Data Protection Board, Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related

applications, versione 2.0, 9 marzo 2021; sulla natura del dato pseudonimizzato per il destinatario, Corte giust., 4 settembre 2025, causa C-413/23 P, GEPD c. SRB.

[10] U.S. Department of Commerce, Bureau of Industry and Security, Commerce Finalizes Rule to Secure Connected Vehicle Supply Chains from Foreign Adversary Threats, 14 gennaio 2025, https://www.bis.gov/press-release/commerce-finalizes-rule-secure-connected-vehicle-supply-chains-foreign-adversary-threats.

[11] Comunicato dello Stato maggiore delle Forze armate polacche (SGWP), 17 febbraio 2026, ripreso integralmente dall'agenzia PAP (TVN24 Biznes, 17 febbraio 2026, https://tvn24.pl/biznes/moto/chinskie-samochody-z-zakazem-wjazdu-na-tereny-wojskowe-decyzja-sztabu-generalnego-obawy-o-bezpieczenstwo-st8906406) e da Defence24, 19 febbraio 2026, https://defence24.pl/sily-zbrojne/chinskie-samochody-nie-wjada-a-co-z-innymi-markami. Il testo originale sul sito dello Stato maggiore non è stato consultato.

[12] NIS Cooperation Group, EU Coordinated Risk Assessment on the Cybersecurity of Connected and Automated Vehicles, 30 gennaio 2026, pp. 2-3 e 36-37, https://ec.europa.eu/newsroom/dae/redirection/document/124122. Testo originale dei passaggi citati: "A supplier can leverage both known and hidden direct access pathways to the vehicle as an attack vector, thereby effectively bypassing many of the controls mandated by the type-approval regulation"; "The type-approval regime was mainly created to ensure traffic safety and does not sufficiently mitigate against such risks." Sulla natura non vincolante, p. 3.

[13] Comitato parlamentare per la sicurezza della Repubblica, Relazione sull'attività svolta, Doc. XXXIV, n. 5, trasmessa alle Presidenze il 4 agosto 2026, p. 35.

[14] Pirelli, Pirelli: new measures to Marco Polo/CNRC by Golden Power PMO Decree, comunicato stampa, 11 aprile 2026, https://corp-assets.pirelli.com/corporate/cs_pirelli_provvedimentogp_aprile2026_eng.pdf, che riporta il contenuto del DPCM del 9 aprile 2026 adottato ai sensi del D.L. 21/2012.

[15] DPCM 30 aprile 2025, GU Serie Generale n. 102 del 5 maggio 2025, allegati 1, 2 e 3 (videosorveglianza: categoria 17; software di controllo dei droni: categoria 22); DPCM 2 ottobre 2025, GU n. 243 del 18 ottobre 2025; DPCM 25 settembre 2014, GU dell'11 dicembre 2014.

[16] "BYD and Yutong to deliver electric buses to Italy", electrive.com, 8 gennaio 2024, https://electrive.com/2024/01/08/byd-yutong-to-deliver-electric-buses-to-italy; Sustainable Bus, https://sustainable-bus.com/news/yutong-byd-win-tenders-bari-taranto-electric-buses. Gli atti di gara non sono stati consultati.

[17] Regolamento (UE) 2024/2847 (Cyber Resilience Act), artt. 2, par. 2, lett. c), 14 e 71, par. 2, http://publications.europa.eu/resource/celex/32024R2847; Regolamento ONU n. 155, parr. 5.1, 6.7, 7.2.2.4 e 7.4.1 e allegato 5, GU L 82 del 9.3.2021, http://publications.europa.eu/resource/celex/42021X0387; Regolamento (UE) 2019/2144, allegato II, http://publications.europa.eu/resource/celex/02019R2144-20260802; Regolamento ONU n. 156, reso obbligatorio dal Regolamento delegato (UE) 2022/2236 che modifica il Regolamento (UE) 2018/858, http://publications.europa.eu/resource/celex/32022R2236. Per gli altri atti della tabella: Direttiva (UE) 2022/2555, http://publications.europa.eu/resource/celex/32022L2555; D.Lgs. 4 settembre 2024, n. 138, https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2024-09-04;138; Regolamento (UE) 2023/2854, http://publications.europa.eu/resource/celex/32023R2854; Direttiva (UE) 2024/2853, http://publications.europa.eu/resource/celex/32024L2853.

[18] Direttiva 2014/53/UE, art. 3, par. 3, lett. d); Regolamento delegato (UE) 2022/30; Regolamento delegato (UE) 2026/339; Direttiva 2010/40/UE, come modificata dalla Direttiva (UE) 2023/2661; Regolamento delegato (UE) n. 886/2013; Regolamento delegato (UE) 2022/670.

[19] Regolamento (UE) 2018/858, art. 6, par. 5, e capo XI (artt. 51-56), testo consolidato, http://publications.europa.eu/resource/celex/02018R0858-20260802.

[20] Corte giust., grande sezione, 22 ottobre 2024, causa C-652/22, Kolin Inşaat Turizm Sanayi ve Ticaret.