IVASS
ISTITUTO PER LA VIGILANZA SULLE ASSICURAZIONI

Convegno AIPSA

Mobilità elettrica: opportunità di business e sfide di sicurezza

Intervento del Consigliere dell'IVASS
Prof. Riccardo Cesari

Roma, 19 maggio 2023

Ringrazio AIPSA, Associazione Italiana Professionisti della Security Aziendale e Di.Gi. Academy per questo invito e soprattutto per aver organizzato un incontro su un tema così importante e lungimirante, sia da un punto di vista strategico sia da un punto di vista tecnologico.

La mobilità è oggi il concentrato e l'avanposto delle ultime tre rivoluzioni industriali: quella dell'elettricità, quella dell'elettronica e quella dell'intelligenza artificiale.

Ma oggi la mobilità elettrica è non solo un'area di potenziali rischi ma anche uno strumento di gestione, di riduzione, a volte di neutralizzazione dei rischi.

Naturalmente *in primis* c'è il fondamentale apporto della mobilità elettrica nella lotta all'inquinamento e ai rischi del cambiamento climatico, grazie a una riduzione del consumo di petrolio che dovrebbe superare i 5 milioni di barili (circa 800 milioni di litri) al giorno nel 2030, con una riduzione annua di inquinanti per circa 700 milioni di tonnellate CO_2-equivalenti (fonte: International Energy Agency). Ma vorrei sottolineare che la diffusione della componentistica digitale e l'installazione di strumenti che consentono la geolocalizzazione del veicolo hanno consentito di ridurre anche molti altri rischi connessi alla mobilità. Ne sono prova alcune inequivocavili tendenze quantitative.

Negli ultimi 20 anni gli incidenti gravi, con lesioni alle persone, sono scesi da 263 mila nel 2001 a 152 mila nel 2021 (-42%); le vittime della strada sono più che dimezzate: da quasi 7100 nel 2001 a 2875 nel 2021 (-60%). Analogamente, la frequenza dei sinistri è scesa in vent'anni dal 12% a meno del 5%.

Nel contempo, tuttavia, sono sorti rischi finora sconosciuti. Mi riferisco, specificamente, ai rischi connessi ai malfunzionamenti degli strumenti, in particolare a quelli prodotti dolosamente.

Tralascio qui tutta la problematica giuridica che si apre con riferimento alle responsabilità e mi concentro solo sulla individuazione dei rischi, anche per sollecitare gli autorevoli presenti, tecnicamente molto più competenti di me, a discutere sulle soluzioni migliori per la minimizzazione questo tipo di rischiosità.

Il problema del malfunzionamento casuale è già noto all'industria automobilistica che negli anni ha trovato il modo per gestirlo e per ridurne al minimo gli effetti negativi. La nuova problematica è determinata da possibili attacchi hacker al veicolo che può essere esso stesso obiettivo dell'attacco ma può anche essere utilizzato come "cavallo di Troia" per attaccare i sistemi che entrano in contatto informatico col veicolo stesso. Non a caso "veicolo" ha la radice latina in *vehere*, "tras-portare", con l'ambigua valenza tanto del portare fuori quanto del portare dentro e del portare attraverso.

I veicoli di ultima, ma anche penultima generazione sono dotati di sistemi digitali che nel continuo o anche soltanto periodicamente si trovano a colloquiare con sistemi esterni e ciò li espone ai rischi di acquisizione e diffusione di "virus patogeni" (in senso informatico), proprio come succede con l'esposizione del corpo umano.

E' necessario pertanto disporre di sistemi che prevengano l'acquisizione dei "virus", ma questo potrebbe non bastare: mi pare infatti assolutamente necessario dotare i veicoli di strumenti che nei casi di superamento delle barriere difensive blocchino il veicolo chiudendo prontamente le porte virtuali di comunicazione con l'esterno.

L'utilizzo malevolo della strumentazione di bordo da parte degli hackers può consentire la consumazione di molteplici reati comuni che non è il caso di enucleare, fino al caso estremo di azioni terroristiche di vasta e deleteria portata.

Mi voglio invece soffermare sull'importanza della difesa del dato di geolocalizzazione.

Oltre alla distorsione per i reati di frode assicurativa, l'accesso illegittimo alla geolocalizzazione agevola la realizzabilità di molti altri reati e, da ultimo, può anche costituire un problema di sicurezza nazionale: si pensi all'ipotesi che i dati sulla geolocalizzazione di veicoli militari o pubblici cadano in mano a potenze militari straniere.

Questo della geolocalizzazione è un rischio a cui è esposta la strumentazione di bordo del veicolo ma anche quella di stazioni riceventi come provider di servizi e gestori di black box installate su veicoli. Queste black box, in base alle nostre rilevazioni IPER, sono ormai stabilmente presenti su più di un quinto del parco auto nazionale (Fig. 1).

FIG. 1 Tasso di penetrazione della scatola nera in Italia (2014-2023)

Cosa comporta tutto ciò per il mercato assicurativo?

Certamente siamo di fronte a una serie di rischi e responsabilità aggiuntive su cui è bene ci sia un ampio confronto: ad esempio mi sembrerebbe utile una certificazione di sicurezza informatica della strumentazione di bordo (sia quella nativa del veicolo, sia quella installata successivamente).

Anche le Autorità di Vigilanza, a cominciare dall'IVASS, sono direttamente interessate al tema dei rischi cyber. Ad esempio qualora si andasse, lo dico in via puramente ipotetica, verso una riforma dell'attuale sistema di bonus/malus che comportasse l'individuazione di un insieme-base di dati informatici sui comportamenti di guida del veicolo, da scambiarsi tra compagnie per la valutazione del rischio e quindi per la determinazione del prezzo della copertura, questi dati andrebbero salvaguardati tanto a difesa dell'assicurato quanto a difesa dell'assicuratore.

Come noto, si conferma anche in questo caso che l'introduzione di nuovi rischi nella vita quotidiana significa anche opportunità di business per chi svolge il mestiere di assicuratore.

A tal proposito è bene, a mio parere, che le compagnie di assicurazione si dotino in fretta delle esperienze e delle competenze necessarie per conoscere, misurare, gestire e infine assicurare correttamente anche questi nuovi tipi di rischi.

Il dibattito di oggi, sono convinto, sarà di grande utilità anche sotto questa prospettiva.

Grazie e auguri di buon lavoro a tutti.