ATTUALITÀ

IVAN SALVADORI

Minacce alla *automotive cybersecurity* e tutela penale della sicurezza dei trasporti

Il contributo ha ad oggetto le minacce cibernetiche per il settore automobilistico. Dopo aver definito il concetto di *automotive cybersecurity*, verranno analizzate le principali iniziative adottate a livello sovranazionale che impongono elevati standard di *cyber*-sicurezza per le *smart cars*. Si verificherà, quindi, se nella legislazione penale italiana esistano norme incriminatrici in grado di contrastare tali minacce. Sarà così possibile stabilire se debbano essere introdotte nuove fattispecie penali per colmare eventuali lacune normative a tutela della sicurezza dei trasporti. In conclusione, si formuleranno alcune proposte per proteggere in modo più efficace la *automotive cybersecurity*.

Automotive cybersecurity threats and criminal protection to transport security.

The paper focuses on the main cyber threats to the automotive sector. It defines the concept of automotive cybersecurity and analyses the supranational legal sources, which impose high cyber-security standards in this field. It also investigates the Italian criminal legislation dealing with cyber-attacks to smart cars and establishes if new criminal offenses should be introduced to fill any regulatory gaps. Finally, some proposals are formulated to guarantee a much more effective protection of the automotive cybersecurity.

1. *Introduzione.* L'industria automobilistica è da tempo soggetta ad una radicale trasformazione dovuta al processo di automazione della guida, dalla espansione della mobilità elettrica (*electromobility*) ed in particolare dalla digitalizzazione e dalla connessione alle reti *wireless* e ad internet dei più moderni veicoli intelligenti (*smart cars*).

Nel prossimo futuro i veicoli connessi ed autonomi (*connected and autonomous vehicles*; di seguito CAV[1]), attualmente in fase di sviluppo e

[1] Per auto connessa si intende, in questo contesto, un veicolo dotato di sistemi di comunicazione, che forniscono l'accesso ad Internet, nonché, di regola, di una rete *wireless* interna, che consente di interconnettere i *device* di cui dispone (ECU, sensori, ecc.) per fornire al conducente ed ai passeggeri

sperimentazione, saranno dotati di tecnologie avanzate e costituiranno sofisticati sistemi c.d. *cyber*-fisici, in grado di raccogliere e trattare, grazie alle tecnologie dell'IA, una enorme mole di dati (sul traffico, sulla rete stradale, sui comportamenti dei conducenti e del veicolo, ecc.), contribuendo così a ridurre i sinistri, il traffico e l'impatto ambientale[2].

Mediante la creazione di apposite *smart roads* e reti veicolari *ad hoc* (*Vehicular ad hoc networks* o VANETs), i CAV potranno essere connessi tra loro (V2V), con l'infrastruttura stradale (V2I) e, più in generale, con il mondo esterno (V2X)[3].

Per l'effettiva immissione sul mercato delle auto a guida completamente autonoma (*fully autonomous cars*) occorrerà attendere, secondo le più rosee aspettative, una decina di anni[4]. Il passaggio verso l'*autonomous driving* è, però, inarrestabile[5].

Le auto a guida automatizzata (di livello 3, secondo gli standard SAE)[6], i c.d. *software-defined vehicles* (SDVs) ed i CAV sono già una realtà ed il loro utilizzo

---

maggiori comfort, servizi (radio, internet, tv, ecc.) ed informazioni (sullo stato del mezzo, notifiche automatiche di collisione, di eccesso di velocità, *alert* di sicurezza, ecc.).

[2] PATIL-MORE-KULKARNI, *A Review on Vehicular Cyber Physical Systems*, in *IRJET*, 2018, 5, 1138 ss.; KUKKALA-PASRICHA, *Machine Learning and Optimization Techniques for Automotive Cyber-Physical Systems*, Berlin, 2023; CONRAD-AL RUBAYE-TSOURDOS, *Intelligent Embedded Systems Platform for Vehicular Cyber-Physical Systems*, in *Electronics*, 2023, 12, 2908 ss.

[3] HUQ-GIBSON-KROPOTOV-VOSSELER, *Cybersecurity for Connected Cars*, TREND Micro, 2021, 5 ss. Sull'impatto dei CAV nel settore automobilistico v. l'analisi di CSA Group, *Connected and Automated Vehicles Codes and Standards Roadmap*, 2021, consultabile al sito *www.csagroup.org/wp-content/uploads/CSA-CAV-Report_Digital-Accessible.pdf*.

[4] Secondo le previsioni più ottimistiche, spesso formulate da aziende con evidenti interessi finanziari nel settore, occorrerà attendere fino al 2030 per vedere in circolazione le *self-driving cars*. Cfr. Globaldata, *Future of Autonomous Vehicles*, 2022. Forti critiche nei confronti di tali previsioni vengono mosse, ad es., da LITMAN, *Autonomous Vehicle Implementation Predictions Implications for Transport Planning*, 2023, consultabile al sito *www.vtpi.org/avip.pdf*. In base ad un recente studio di McKinsey & Company, si stima che nel 2030 il 15% delle auto immatricolate saranno a guida autonoma ed il 55% a guida semi-autonoma, per un totale di 200 milioni di veicoli (v. McKinsey & Co., *Autonomous driving's Future: Convenient and Connected*, 2023).

[5] Si stima che il mercato dei SDV passi dai 36 miliardi di dollari del 2022 a oltre 210 miliardi di dollari nel 2032, con una crescita media annua pari al 19%. Cfr. Precedent Research, *Software-defined vehicles Market Size, Share, and Trends 2024 to 2034*, 2024, consultabile al sito *www.precedenceresearch.com/software-defined-vehicles-market*.

[6] Ad inizio del 2022, la Mercedes-Benz iniziò a produrre, nell'ambito del segmento premium (S-Class e EQS), auto a guida autonoma condizionata (di livello 3, secondo gli standard SAE). Il sistema Drive Pilot ADAS, installato su questi modelli, in determinate condizioni metereologiche e di traffico (ad es. in

sulle strade pubbliche è destinato ad aumentare nei prossimi anni, venendosi progressivamente a sostituire al vecchio comparto auto.

La struttura elettromeccanica dei veicoli tradizionali è connotata da una architettura chiusa, che non prevede comunicazioni con l'esterno. Di contro, le *smart cars* poggiano su un complesso ed articolato ambiente aperto, composto da centinaia di componenti elettronici, da ECU (*electronic central unit*) e *micro-chip*, prodotti in diversi Paesi, da interfacce di comunicazione con servizi esterni (Bluetooth, WI-FI, LTE, LIn), gestiti da *Provider* esterni, da sofisticati algoritmi e sensori (LIDAR), da sistemi informatici di bordo e da servizi di *infotainment* costantemente aggiornati mediante sistemi *over-the-air* (OTA)[7]. Di conseguenza, il corretto funzionamento e la sicurezza dei moderni veicoli automatizzati dipendono in grande misura dalla integrità e dalla resilienza delle numerose e complesse parti *hardware* e *software* di cui sono composti[8].

Per la loro architettura elettronica e *software-oriented*, le *smart cars* sono particolarmente vulnerabili ai sempre più insidiosi *cyber-attacks*[9]. Ulteriori rischi per la sicurezza dei moderni *computers on wheels* derivano dalle

---

autostrada), possono svolgere autonomamente alcune funzioni di guida (sterzare, accelerare e frenare o cambiare corsia), anche se il conducente deve tenersi pronto a riprendere in qualsiasi momento il controllo del veicolo, quando il sistema lo richieda. Tali modelli sono stati i primi al mondo ad essere omologati in conformità con il Regolamento UNICE n. 156 (v. *infra*, par. 4.1). Nello stesso anno, la casa automobilistica di Stoccarda ottenne l'autorizzazione da parte delle autorità tedesche per mettere in circolazione questi modelli. Anche la BMW ha di recente installato, sulla sua serie 7, il sistema di guida automatizzata di livello 3, che prende il nome di Personal Pilot L3: esso funziona soltanto su determinate strade e con una velocità massima di 60 km/h. Questi modelli possono essere utilizzati, al momento, solo in Germania, avendo ottenuto le necessarie autorizzazioni.

[7] V. SUDHAKAR-SZE-KARAMAN, *Data Center on Wheels: Emission from Computing on Board Autonomous Vehicles*, in *IEEE MICRO Special Issue on Environmentally Sustainable Computing*, 2022, 1 ss.; IGNATIOUS-EL SAYED-KHAN, *An Overview of Sensors in Autonomous Vehicles*, in *Procedia Computer Science*, 2022, 198, 736 ss.

[8] V. *infra*, par. 5.

[9] WEIMERSKIRCH-DOMINIC, *Assessing Risk: Identifying and Analyzing Cybersecurity Threats to Automated Vehicles*, U. Mich. White Paper, 2018, consultabile al sito *www.mcity.umich.edu/wp-content/uploads/2017/12/Mcity-white-paper_cybersecurity.pdf*; PAVITHRA-KALIAPPAN-RAJENDAR, *Security Algorithm for Intelligent Transport System in Cyber-Physical Systems Perceptive: Attacks, Vulnerabilities, and Countermeasures*, in *SN Computer Science*, 2023, 4, 544 ss. V. anche il considerando 26 de Regolamento UE 2019/2144: «*the connectivity and automation of vehicles increase the possibility for unauthorized remote access to in-vehicle data and the illegal modification of software over the air*».

peculiari caratteristiche dell'industria automobilistica, la quale poggia su una complessa *supply chain*, composta da un ampio reticolo di aziende ed imprese che operano in molteplici settori (meccatronica, IT, IA, ecc.)[10].

La catena di distribuzione nel settore dell'*automotive* ricomprende, oltre al produttore del veicolo (*Original Equipment Manufacturer*: di seguito OEM), i fornitori di singoli moduli o sistemi (ad es. *engine control unit*, *infotainment module*, ecc.) e componenti (*microchip*, sensori, microcircuiti, ecc.), nonché diversi *Service Providers* e reti (*wireless*, internet, ecc.), gestiti da soggetti terzi.

L'intervento, in questa complessa organizzazione, di numerosi soggetti (persone fisiche e giuridiche), che operano in diversi Stati, contribuisce a rendere il sofisticato ecosistema di un veicolo intelligente maggiormente vulnerabile alle minacce informatiche. Queste ultime possono, infatti, colpire non solo i numerosi sensori e *software* da cui dipende il loro corretto funzionamento, ma anche le reti di comunicazione con i dispositivi interni e con i c.d. *backend servers* dei produttori e venditori[11].

I menzionati attacchi cibernetici, oltre a mettere in pericolo la sicurezza del traporti, possono ledere l'integrità fisica e la vita del conducente, dei passeggeri e di tutti coloro che sono coinvolti nella circolazione stradale (pedoni, ciclisti, ecc.)[12].

La dottrina penalistica più attenta alle sfide connesse con la rivoluzione tecnologica ed all'impatto dell'IA nel settore dei trasporti, si è, ad oggi, concentrata in particolare sui profili giuridici legati alla guida autonoma e sull'individuazione dei criteri di imputazione per (potenziali) eventi lesivi causati dalle (future) *self driving cars*[13]. Scarsa attenzione è stata rivolta, invece,

---

[10] WTW, *Global Automotive Risk Outlook 2024*, 2024, 17, consultabile al sito *www.andaf.it/media/380543/global-automotive-risk-outlook-2024.pdf.*

[11] Cfr. Kaspersky Ics Cert, *Cybersecurity in the automotive industry: Ensuring compliance with UNICE Regulations*, Version 1.0. 2024, consultabile al sito *www.ics-cert.kaspersky.com/publications/reports/2024/02/07/cybersecurity-in-the-automotive-industry-ensuring-compliance-with-unece-regulations/.*

[12] Cfr. GUAN-HAN-KANG-TANG-CHEN-WANG, *An Overview of Vehicular Cybersecurity for Intelligent Connected Vehicles*, in *Sustainability*, 2022, 14, 1 ss.

[13] Nella ormai copiosa letteratura penale italiana v., per tutti, CAPPELLINI, *Profili penalistici delle self-driving cars*, in *Dir. pen. cont.*, 2019, 2, 326 ss.; PICOTTI, *Profili di responsabilità penale per la circolazione di veicoli a guida autonoma*, in *Studi in onore di Antonio Fiorella*, a cura di Catenacci-D'Ascola-Rampioni, Roma, 2021, vol. I, 813 ss.; ed in particolare lo studio monografico di LANZI, *Self-*

agli aspetti, tutt'altro che secondari, concernenti la tutela (anche) penale della *automotive cybersecurity*.

Nel presente contributo, dopo aver dato conto della rappresentazione mediatica delle minacce cibernetiche per le *smart cars* (par. 2), si provvederà a definire il concetto di *cybersecurity* nel settore automobilistico (par. 3). Verranno richiamate le più recenti iniziative adottate a livello sovranazionale per implementare la (*cyber*)sicurezza dei veicoli intelligenti, valutandone l'adeguatezza a prevenire potenziali cyber-attacchi (par. 4). Si analizzeranno, quindi, le principali minacce per l'*automotive cybersecurity* e si verificherà la loro rilevanza penale nel nostro ordinamento (par. 5). Sarà così possibile accertare l'esistenza di eventuali lacune normative tali da giustificare, *de lege ferenda*, l'introduzione di nuovi reati per tutelare l'integrità ed il corretto funzionamento delle *smart cars* e, più in generale, la sicurezza dei trasporti (par. 6). In conclusione, si formuleranno alcune concrete proposte per implementare la *cybersecurity* in questo ambito (par. 7).

2. *La rappresentazione mediatica delle* cyber*-minacce alle smart cars.*

L'esistenza di un oggettivo e preoccupante rischio cibernetico nel settore dei trasporti, ed in specie per i veicoli intelligenti, trova conferma in alcune recenti ed autorevoli ricerche[14]. Tuttavia, la reale entità di tale minaccia per il comparto automobilistico viene spesso sovrastimata e rappresentata in modo alquanto allarmistico[15].

Nel favorire il consolidarsi di una percezione distorta delle *cyber*-minacce nell'ambito dei trasporti rilevante è, senza dubbio, il ruolo dei *mass-media*. Frequenti sono gli *scoop* giornalistici che danno per imminente la messa in

driving cars e responsabilità penale. La gestione del "rischio stradale" nell'era della intelligenza artificiale, Torino, 2023, *passim*, cui si rinvia per ampi riferimenti bibliografici; in quella di lingua tedesca v., ad es., GLESS, *Strafrechtliche Aspekte der Fahrautomatisierung (Beispiel Parkassistenz) – Wird der Mensch zur Knautschzone für das Auto?*, in *Jahrbuch zum Strassenverkehrsrecht*, a cura di Landolt-Dähler, Zürich, 2022, 337 ss.; ID., *„Mein Auto fuhr zu schnell, nicht ich!" – Strafrechtliche Verantwortung für hochautomatisiertes Fahren*, in *Intelligente Agenten und das Recht*, a cura di Gless-Seelmann, Baden-Baden, 2016, 225 ss.

[14] V., ad es., Kaspersky Ics Cert, *Cybersecurity*, cit., 1 ss.

[15] Cfr. MCLACHLAN-SCHAFER-DUBE-KYRIMI-FONTON, *Tempting the Fate of the Furious: Cyber Security and Autonomous Cars*, in *Int'l Review of Law, Computers and Technology*, 2022, 36, 181 ss., 182.

circolazione sulle strade pubbliche delle *self-driving cars*, prospettando, al contempo, scenari apocalittici per la *smart mobility*, come conseguenza di pericolosissimi *cyber*-attacchi. Molto spesso, però, si tratta di notizie che non trovano riscontro in evidenze oggettive o che non sono supportate da studi scientifici.

Ricorrente è il richiamo, da parte di molti mezzi di informazione, a previsioni (spesso volutamente) allarmistiche, formulate in specie da alcune compagnie assicurative, nonché ai proclami di carismatici leader di case automobilistiche, i quali sono mossi da evidenti finalità di *marketing*[16]. Non stupisce pertanto se nell'opinione pubblica e, talora, tra alcuni addetti ai lavori, facciano particolare presa scenari catastrofici degni delle migliori serie televisive di genere fantascientifico e delle produzioni cinematografiche hollywoodiane.

La realtà lascia spesso spazio all'immaginazione: *autonomous cars* fuori controllo che investono pedoni; pericolosi *hacker* che prendono il controllo di intere flotte di *smart cars*, mandando in tilt il traffico delle grandi città e cagionando spaventosi incidenti a catena; spietati *cyber*-terroristi che sequestrano i passeggeri delle auto senza pilota o intenzionati a cagionare stragi, lanciando i CAV a tutta velocità contro la popolazione[17].

Ad alimentare ingiustificate paure per il rapido sviluppo tecnologico che connota il settore *automotive* sono, in alcuni casi, anche articoli scientifici e report di autorevoli istituzioni internazionali, i quali, anziché dar conto di *cyber*-attacchi realmente verificatisi, si concentrano su minacce e scenari che, ad oggi, sono soltanto futuribili o la cui effettiva probabilità di verificazione è alquanto incerta (se non remota)[18].

---

[16] *Ibid.*

[17] V., ad es., VIVEK-YANNI-YUNKER-SILVERBERG, *Cyberphysical Risks of Hacked Internet-Connected Vehicles*, in *Physical Review*, 2019, 100, 1 ss.; RYAN, *The Future of Transportation: Ethical, Legal, Social and Economic Impacts of Self-Driving Vehicles in the Year 2025*, in *Science and Engineering Ethics*, 2020, 26, 1185 ss.

[18] Paradigmatico, in tal senso, il report di ENISA, *Cybersecurity Challenges in the Uptake of Artificial Intelligence in Autonomous Driving*, 2021, consultabile al sito *www.enisa.europa.eu/publications/enisa-jrc-cybersecurity-challenges-in-the-uptake-of-artificial-intelligence-in-autonomous-driving*. In dottrina v., ad es., MEYER-ELVIK-JOHNSSON, *Risk Analysis for Forecasting Cyberattacks against Connected and Autonomous Vehicles,* in *Journal of Transportation Security*, 2021, 227 ss.

Essendo ancora lontani dalla effettiva messa in circolazione delle *fully autonomous cars* (livello 5 e 6 SAE), pare alquanto difficile, se non impossibile, stabilire, allo stato attuale, le probabilità del verificarsi di incidenti e disastri causati da (potenziali) *cyber*-attacchi in questo settore[19].
Focalizzarsi soltanto sui rischi che potrebbero sorgere in futuro, quando, secondo le previsioni, la circolazione stradale sarà dominata dalle auto autonome e dai CAV, rischia di essere, allo stato attuale, un mero esercizio speculativo. Un eccessivo (e spesso ingiustificato) allarmismo potrebbe inoltre favorire l'adozione, a livello internazionale e nazionale, di discutibili scelte (anche politico-criminali) basate su una percezione distorta del rischio, anziché sul reale substrato empirico-criminologico. Ma così facendo, si finirebbe per ostacolare lo sviluppo delle *smart cars*, a vantaggio dei Paesi dove la loro sperimentazione è già molto avanzata (come, ad es., in Cina o negli Stati Uniti)[20].

3. La nozione di cybersecurity *in ambito automobilistico.* Per individuare le reali *cyber*-minacce per il settore dei trasporti e verificare, al contempo, l'efficacia delle strategie adottate a livello sovranazionale per garantire un elevato livello di sicurezza informatica *in subjecta materia*, è necessario definire preliminarmente il significato di *automotive cybersecurity*.
La definizione di *cybersecurity* è molto controversa anche tra gli addetti ai lavori e varia a seconda del settore (informatico, IT, giuridico, *intelligence*, ecc.) in cui tale concetto viene impiegato[21].

Cfr. MCLACHLAN-SCHAFER-DUBE-KYRIMI-FONTON, *Tempting the Fate of The Furious*, cit., 183, i quali evidenziano come vi sia una convergenza in questo ambito tra le inchieste giornalistiche ed i dati richiamati da ampi settori della letteratura accademica, i quali si fanno spesso influenzare dalle prime; ma in questo modo si contribuisce a creare una immagine distopica, anziché contribuire a fornire un quadro delle reali minacce cibernetiche per il comporto dell'*automotive*.

[19] *Ibid.*

[20] *Ibid.*

[21] Cfr. FUSTER-JASMONTAITE, *Cybersecurity Regulation in The European Union: The Digital, The Critical and Fundamental Rights*, in CHRISTEN-GORDIJN-LOI, *The Ethics of Cybersecurity: The International Library of Ethics, Law and Technology*, Cham, 2020, 97 ss.; PAPAKONSTANTINOU, *Cybersecurity as Praxis and as a State: The EU Law Path towards Acknowledgement of a New Right to Cybersecurity?*, in *Computer Law & Security Review*, 2022, 44, 1 ss., 2-3; CEN/CENELEC CSCG, *Recommendation #2 – Definition of Cybersecurity*, v. 01.08, 2020, p. 1 ss., p. 11 ss.; IET, *Automotive*

Secondo un primo orientamento, la *cybersecurity* andrebbe intesa come "attività" (*praxis*), vale a dire come l'insieme delle azioni, delle misure e dei procedimenti da adottare in un determinato ambito per proteggerlo da potenziali attacchi cibernetici[22]. Paradigmatica, in tal senso, è la definizione di *vehicle cybersecurity* elaborata dall'*Automotive Information Sharing and Analysis Center* (Auto-Isac): «*the activities, processes, and capabilities that protect, detect, and respond to cybersecurity occurrences (e.g. remote control, unauthorized access, disruption, manipulation) that actually or potentially result in adverse consequences to a vehicle, connected infrastructure, or information that the vehicle processes, stores, or transmits*»[23].

Analogo è l'approccio adottato, a livello europeo, con il *Cybersecurity Act* del 2019, il quale definisce, in senso più ampio, la *cybersecurity* come «*l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche*» (art. 2.1)[24].

Da una diversa prospettiva, la *cybersecurity* andrebbe concepita come uno stato (*state*), una condizione o livello di protezione, che verrebbe raggiunto con l'adozione di azioni, misure e procedure volte a proteggere i veicoli da ogni forma di minaccia cibernetica[25]. In altre parole, la cibersicurezza verrebbe a costituire un ambito protetto da ogni forma di *cyber*-attacco, di cui gli individui, le persone giuridiche e, più in generale, la collettività hanno il diritto di disporre per svolgere in modo sicuro le loro attività (personali, sociali, economiche, professionali, ecc.)[26]. La *cybersecurity*, in tale ottica, assurgerebbe al rango di

---

Cyber Security: An IET/KTN Thought Leadership Review of Risk Perspectives for Connected Vehicles, 2020, 5.

[22] PAPAKONSTANTINOU, *Cybersecurity*, cit., 1 ss., 2, 4 s.

[23] In senso analogo v. la definizione fornita dalla *Society of Automotive Engineering* (SAE): «*the technologies, processes and controls designed to protect vehicle systems, networks, programs and data against criminal or unauthorized use*».

[24] In dottrina v. DIETMAR-MÖLLER-HAAS, *Guide to Automotive Connectivity and Cybersecurity. Trends, Technologies, Innovations and Applications*, Cham, 2018. Nel nostro ordinamento v. il recente d.lgs. 4 settembre 2024, n. 138 di recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148. L'art. 2, co. 1, lett. r) reg. cit. definisce la sicurezza informatica come «l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche [...]».

[25] PAPAKONSTANTINOU., *Cybersecurity*, cit., 2.

[26] PAPAKONSTANTINOU, *Cybersecurity*, cit., 6.

bene giuridico collettivo, meritevole e bisognoso di essere protetto anche mediante lo strumento penale[27].

Nel settore automobilistico pare più corretto definire la sicurezza cibernetica come una condizione[28]. Essa va intesa cioè come il necessario livello di protezione che deve essere raggiunto, attraverso l'adozione di specifiche strategie, procedimenti, standard e misure, di natura non solo tecnico-informatica, ma anche giuridico-penale, per proteggere da potenziali *cyber*-attacchi i dati informatici, i *software*, i dispositivi ed i sistemi informatici da cui dipende il corretto e sicuro funzionamento dei veicoli intelligenti.

Tale impostazione è stata adottata anche dal Forum mondiale delle Nazioni Unite per l'armonizzazione delle regolamentazioni sui veicoli (di seguito WP.29), al quale compete garantire l'aggiornamento dei requisiti tecnici dei veicoli. Il WP.29 definisce l'*automotive cybersecurity* come «la condizione in cui i veicoli stradali e le loro funzioni sono protetti da minacce informatiche nei confronti dei componenti elettrici o elettronici»[29].

Il raggiungimento, in questo specifico ambito, di elevati standard di *cybersecurity*, oltre ad assicurare l'efficienza e la sicurezza dei veicoli e dei trasporti, tutela maggiormente i fruitori delle *smart cars* e coloro che sono coinvolti nella circolazione stradale (passeggeri, pedoni, ecc.)[30]. Ma il conseguimento di tale obiettivo richiede il necessario coinvolgimento delle molteplici persone fisiche (programmatori, sviluppatori, produttori, venditori, ecc.) e giuridiche (aziende, multinazionali, case automobilistiche, ecc.) che intervengono nella complessa *supply chain* del settore *automotive*. Solo in questo modo è, infatti, possibile, garantire che gli standard di sicurezza, previsti a livello sovranazionale ed interno, si applichino a ciascun veicolo e ad ogni suo

---

[27] Sul bene giuridico della sicurezza informatica v. PICOTTI, *Sicurezza, informatica e diritto penale*, in *Sicurezza e diritto penale*, a cura di Donini-Pavarini, Bologna, 2011, 217 s.; volendo anche SALVADORI, *L'accesso abusivo ad un sistema informatico o telematico. Una fattispecie paradigmatica dei nuovi beni giuridici emergenti nel diritto penale dell'informatica*, in *Tutela penale della persona e nuove tecnologie*, a cura di Picotti, Padova, 2013, 125 ss.; ID., *I reati contro la riservatezza informatica*, in *Cybercrime*[2], a cura di Cadoppi-Canestrari-Manna-Papa, Torino, 2023, 694 ss., 702 ss.

[28] Cfr. VELLINGA, *Connected and vulnerable*, in *International Review of Law, Computers & Technology*», 2022, 36, 161 ss., 162.

[29] Art. 2.2 regolamento n. 155 UNECE (v. *infra*, par. 4.1).

[30] Cfr. Center of Automotive Management, *Automotive Cyber Security*, White paper, 2023, 6.

componente (elettrico, elettronico, informatico, ecc.), fin dalla iniziale fase di sviluppo, nonché alle infrastrutture di supporto (*server* per l'aggiornamento del *firmware* delle ECU, reti di comunicazione con i sistemi di *infotainment*, ecc.) ed a quelle delle case automobilistiche.

Per proteggere i veicoli da potenziali attacchi informatici occorre adottare procedure e misure di sicurezza tali da garantire la riservatezza, la disponibilità e la integrità (c.d. *CIA triad*), la resilienza, l'autenticità e l'affidabilità dei componenti elettronici, dei dati, dei sistemi informatici e delle reti che compongono il complesso ecosistema delle moderne auto intelligenti[31].

La prevenzione degli accessi non autorizzati (*hacking*), dei danneggiamenti dei sistemi informatici (mediante *malware*, *ransomware*, attacchi DoS, ecc.) e delle intercettazioni illecite di dati informatici (attraverso *spyware*, *Trojan Horse*, ecc.), che rischiano di compromettere l'efficienza e la resilienza dei veicoli intelligenti e, più in generale, la sicurezza dei trasporti, passa innanzitutto attraverso l'adozione di misure volte a garantire la riservatezza informatica (*confidentiality*)[32].

La protezione dell'integrità dei dati, dei sistemi di informazione, del c.d *controller area network* (CAN) *bus* e delle molteplici componenti elettroniche ed informatiche di cui sono sono dotate le *smart cars* consente di assicurare la loro affidabilità ed il corretto funzionamento dei processi di *decision-making* automatizzati o semi-autonomi. La tutela della loro integrità (*integrity*) costituisce il presupposto per garantire l'autenticità, l'accuratezza e la consistenza dei dati, dei sistemi informatici e dei componenti elettronici di un veicolo intelligente durante il suo intero ciclo di vita.

Ma l'efficacia e l'efficienza dei sistemi informatici dipendono altresì dalla disponibilità ed efficacia (*availability*) delle loro funzioni e dalla loro capacità di svolgere le operazioni (di guida e frenata assistita, ecc.) per cui sono stati

---

[31] Cfr. GIANNAROS-KARRAS-THEODORAKOPOULOS-KARRAS-KRANIAS-SCHIZAS-KALAGERATOS-TSOLIS, *Autonomous Vehicles: Sophisticated Attacks, Safety Issues, Challenges, Open Topics, Blockchain, and Future Directions*, in *J. Cybersecur. Priv.*, 2023, 493 ss., 497 s. A fianco del concetto di c.d. CIA Triad, quale presupposto per raggiungere una efficace protezione della *cyber-security*, l'Unione europea, in alcuni suoi recenti documenti ufficiali, ha sottolineato l'importanza di tutelare anche la resilienza e l'autenticità dei beni informatici.

[32] V. *infra*, par 5.

elaborati. Di conseguenza, ogni compromissione della disponibilità dei dati, dei sistemi informatici e delle nuove tecnologie dell'IA di cui sono dotati i veicoli più moderni può avere significative conseguenze negative sul piano della sicurezza dei trasporti[33].

4. *Il quadro normativo sovranazionale.* L'aumento della consapevolezza dei *cyber*-rischi per i veicoli intelligenti e per la circolazione stradale ha portato all'adozione, in seno alle Nazioni unite (par. 4.1) ed alla Unione europea (par. 4.2), di importanti misure per implementare la *cybersecurity* nel settore dei trasporti. Numerosi sono altresì gli standard tecnici elaborati, di recente, dalle più autorevoli organizzazioni internazionali che operano nel settore dell'*automotive* (par. 4.3).

4.1. *I regolamenti UNICE n. 155 e n. 156.* La Commissione economica per l'Europa delle Nazioni Unite (UNECE) ha adottato due importanti regolamenti per implementare l'*automotive cybersecurity*[34].
L'obbligo di rispettare gli specifici criteri di sicurezza e di controllo previsti dai citati regolamenti è stato esteso, a partire da luglio 2022, a tutti i nuovi veicoli di nuova omologazione immessi dalle case automobilistiche sul mercato dell'Unione europea; in relazione alla vendita di veicoli di nuova fabbricazione esso è scattato dal 7 luglio 2024[35].
L'art. 7.2.1 del regolamento n. 155 UNECE, recante «disposizioni uniformi relative all'omologazione dei veicoli per quanto riguarda la cibersicurezza e i sistemi di gestione della cibersicurezza», ed entrato in vigore il 22 gennaio 2021, richiede all'OEM del veicolo l'adozione, per il suo intero ciclo di vita (dalla fase di sviluppo, alla produzione ed alla post-produzione), di un sistema di gestione della cibersicurezza (*Cyber Security Management System* o CSMS).

[33] V. *infra*, par. 6.
[34] Per un'analisi delle menzionate iniziative v. VELLINGA, *Connected and Vulnerable*, cit., 162 ss.
[35] Gli elevati costi di adeguamento dei veicoli esistenti ai nuovi standard europei, entrati in vigore da luglio 2024, hanno fatto sì che alcune case automobilistiche abbiano deciso di ritirare dal commercio alcuni loro modelli. È il caso, ad es., del suv Macan della Porsche. La casa automobilistica di Stoccarda ha dichiarato che provvederà a limitarne la vendita soltanto negli Stati Uniti, dove non si applicano gli elevati standard di *cybersecurity* del reg. 155 UNECE (v. *infra*, par. 4.1).

Il CSMS viene definito come un «approccio sistematico basato sul rischio che definisce i processi organizzativi, le responsabilità e la governance per il trattamento dei rischi associati alle minacce informatiche nei confronti dei veicoli e per la protezione degli stessi dagli attacchi informatici» (art. 2.3 reg. n. 155).

La conformità del CSMS agli standard previsti dal reg. n. 155 cit. deve essere accertata dalla competente autorità di omologazione; la sua corretta adozione da parte delle case automobilistiche è, dunque, il presupposto per ottenere l'omologazione dei tipi di veicolo da esse prodotti (art. 5 reg. cit.).

L'ottenimento del certificato di conformità del CSMS costituisce il requisito per la loro messa in circolazione e per il loro utilizzo sulle strade pubbliche (art. 7.2.1)[36]. A tal fine, il produttore del veicolo deve dimostrare di aver adottato adeguate misure di *cybersecurity* già in fase di progettazione del veicolo e durante tutto il suo ciclo di vita (*end-to end security*).

In base al reg. n. 155 cit. i processi organizzativi impiegati dall'OEM, e definiti nel CSMS, devono prevedere una corretta identificazione, valutazione e gestione del rischio (*risk assessment* e *risk management*), nonché la realizzazione di test per verificare la cibersicurezza di ciascun tipo di veicolo. L'obiettivo è di garantire che le minacce informatiche e le vulnerabilità alle quali potrebbe essere soggetto un veicolo, durante il suo *life cycle*, siano attenuate entro un lasso di tempo ragionevole (art. 7.2.2.3 reg. cit.). Ed in tal senso, ogni automobile deve essere in grado di rilevare e rispondere ai possibili *cyber*-attacchi (art. 5.1.1.1., lett. d, reg. cit.). Il regolamento non specifica, tuttavia, quale tipo di risposta dovrebbe essere data nel caso in cui il veicolo subisse un concreto attacco.

Le menzionate misure, come emerge dall'allegato V al reg. n. 155, perseguono l'obiettivo di ridurre i rischi cibernetici nel settore automobilistico per la

[36] In argomento v. DE VINCENZI-COSTANTINO-MATTEUCCI-FENZI-PLAPPERT-RIEKE-ZELLE, *A Systematic Review on Security Attacks and Countermeasures in Automotive Ethernet*, in *ACM Computing Surveys*, 2024, 56, 1 ss., 27 s.

riservatezza, l'integrità e la disponibilità dei dati e dei sistemi informatici di cui sono dotati i nuovi veicoli[37].

Altrettanto importante, in questo contesto, è il regolamento UNECE n. 156, recante «disposizioni uniformi relative all'omologazione dei veicoli per quanto riguarda gli aggiornamenti del software e il relativo sistema di gestione». L'art. 6 reg. n. 156 cit. prevede l'obbligo per il costruttore del veicolo di conseguire il certificato di conformità del sistema di gestione degli aggiornamenti del *software* (SUM).

Il SUM deve definire le procedure ed i processi organizzati adottati dal costruttore per adempiere alle prescrizioni relative alla fornitura degli aggiornamenti dei *software*, stabilite dal menzionato regolamento (art. 2.5 reg. n. 166 cit.).

Al fine dell'ottenimento del certificato di conformità del SUM, il costruttore del veicolo deve dimostrare, analogamente a quanto previsto per il CSMS, di aver adottato processi organizzativi in grado di identificare eventuali interdipendenze del sistema aggiornato con altri sistemi (art. 7.1.5 reg. n. 166 cit.), nonché la compatibilità di un aggiornamento del *software* con la configurazione del veicolo o dei veicoli destinatari prima del suo rilascio.

Il costruttore deve altresì valutare la compatibilità dell'aggiornamento con l'ultima configurazione *software/hardware* nota del veicolo o dei veicoli destinatari, prima del rilascio dell'aggiornamento. In questo modo, si intende implementare il livello di sicurezza dei sistemi informatici di cui sono dotati i moderni veicoli, rispetto alle *cyber*-minacce.

La previsione dell'obbligo, in capo al costruttore del veicolo, di dotarsi di un adeguato sistema di gestione della cibersicurezza (CSMS) e degli aggiornamenti del *software* (SUMS) fa sì che la *cybersecurity* assurga a componente essenziale dei veicoli durante il loro intero ciclo di vita.

Qualora i veicoli non rispettino i menzionati standard di sicurezza, le autorità competenti possono ritirare il certificato di conformità e, di conseguenza, impedire la circolazione del veicolo oggetto di attacco.

---

[37] Sull'importanza di tutelare la sicurezza delle informazioni (*information security*) v. anche lo standard ISO 27001 (*infra*, par. 4.3).

I suddetti regolamenti hanno forza vincolante a livello europeo, dal momento che il regolamento 2019/2144 rinvia, ai fini della omologazione dei veicoli, alla regolamentazione adottata dalla UNECE[38]. Essi scontano, però, un limite oggettivo.

Pur imponendo ai produttori di veicoli di prevenire, durante l'intero *life cycle* di un veicolo, i rischi per la cibersicurezza, i regolamenti UNICE n. 155 e 156 non prevedono, tuttavia, specifiche misure e procedure idonee a proteggere le parti critiche di un veicolo dagli attacchi *cyber*. Nessuna specifica disposizione è invero contemplata per imporre al costruttore l'isolamento delle parti (*software*) critiche dei veicoli dai sistemi informatici di *infotainment*[39]. Tantomeno si stabilisce quando il costruttore dovrebbe rilasciare l'aggiornamento dei *software*, da cui dipende il corretto e sicuro funzionamento dei veicoli. La concreta individuazione, tutt'altro che semplice, di tali misure ed adempimenti, è, di conseguenza, rimessa alle autorità nazionali.

4.2. *Le iniziative adottate dall'Unione europea.* Il primo importante intervento europeo a tutela della *cybersecurity* si è avuto con la direttiva 2016/1148/UE, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione europea (di seguito direttiva NIS), che è stata successivamente abrogata dalla direttiva UE 2022/2555 (c.d. direttiva NIS 2), recante misure per un livello comune elevato di cibersicurezza nell'Unione[40].

[38] V., in tal senso, le modifiche apportate dal regolamento di esecuzione 2022/1426/UE del 5 agosto 2022, recante modalità di applicazione del regolamento (UE) 2019/2144 del Parlamento europeo e del Consiglio per quanto riguarda procedure e specifiche tecniche uniformi per l'omologazione del sistema di guida automatizzata di veicoli completamente automatizzati, il quale, nell'aggiornare la disciplina europea di omologazione dei veicoli, fa espresso riferimento ai regolamenti UNECE n. 155 e 156 (v. *infra*, par. 4.2).

[39] Cfr. VELLINGA, *Connected and Vulnerable,* cit., 166. Di contro gli standard ISO/SAE 21434 prevedono un approccio olistico per definire i rischi in materia di *cybersecurity*, considerata come parte integrante dell'intero ciclo di vita, da parte dei produttori dei veicoli (v. *infra*, par. 4.3).

[40] MARKOPOULOU-PAPAKONSTANTINOU-DE HERT, *The New EU Cybersecurity Framework: The NIS Directive, ENISA's Role and the General Data Protection Regulation*, in *Computer Law and Security Review*, 2019, 35, 1 ss. La direttiva NIS 2, entrata in vigore il 17 gennaio 2023, collocandosi nell'ambito della strategia europea sulla *cybersecurity*, viene ad integrarsi con il quadro normativo europeo in materia di protezione dei dati personali e con la direttiva 2022/2557/UE sulla resilienza dei soggetti critici, tra i quali vengono richiamati anche i servizi intelligenti di trasporto.

Nel definire un quadro comune europeo in materia di cibersicurezza, la direttiva NIS 2, al pari della precedente, include, tra i settori ad alta criticità, il trasporto su strada e, tra i settori critici, la fabbricazione di autoveicoli, ai sensi dell'art. 5, lett. d) dell'allegato II. Di conseguenza, anche coloro che operano nell'ambito dei trasporti, ed in specie dei c.d. *intelligent transport systems* (ITS)[41], sono tenuti, in forza dell'art. 21, par. 1 della direttiva NIS 2, ad adottare misure tecniche ed organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza delle reti e dei sistemi informativi utilizzati nelle loro operazioni, in modo da assicurare un livello di sicurezza adeguato al rischio esistente.

Si prevede inoltre l'obbligo di adottare misure adeguate per prevenire e minimizzare l'impatto di incidenti a carico della sicurezza della rete e dei sistemi informativi utilizzati per la fornitura di servizi essenziali, al fine di assicurare la loro continuità e notificare alle competenti autorità gli incidenti aventi un impatto rilevante sulla corretta erogazione dei servizi essenziali prestati (art. 21, par. 3, dir. cit.).

Nell'assicurare un elevato standard di sicurezza nelle reti e dei sistemi informatici, la direttiva NIS 2 acquista un ruolo fondamentale in relazione alla protezione delle comunicazioni che consentono la connessione tra veicoli (V2V), con la rete di infrastrutture (V2I) e con l'ecosistema che li circonda (V2X). La direttiva contribuisce, infatti, a rafforzare la prevenzione contro gli accessi non autorizzati ai sistemi informatici dei veicoli intelligenti e, dall'altro, a limitare le conseguenze negative che possono derivare al settore dell'*automotive*[42].

Importanti disposizioni in materia di *cybersecurity* sono contenute anche nel già citato regolamento sulla cibersicurezza 2019/881/UE. Esso prevede, in particolare, un sistema europeo di certificazione della cibersicurezza in relazione a ciascun elemento o gruppo di elementi di una rete o di un sistema

[41] Sulla disciplina europea in materia di sistemi intelligenti di trasporto v. Direttiva 2010/40/UE, che contiene il quadro generale per la diffusione dei sistemi di trasporto intelligenti nel settore del trasporto stradale e nelle interfacce con altri modi di trasporto, e che è stata di recente modificata dalla direttiva 2023/2661/UE del 22 novembre 2023.

[42] Cfr. VELLINGA, *Connected and Vulnerable,* cit., 170.

informatico (c.d. prodotti TIC)[43]. Dato che il menzionato regolamento europeo non fa espresso riferimento all'ambito dei trasporti, non è chiaro se per prodotti TIC si debbano intendere anche le parti *hardware* e *software* che compongono un veicolo intelligente.

La direttiva UE 2022/2557, relativa alla resilienza dei soggetti critici, e che abroga la direttiva 2008/114/CE, richiama tra i suoi destinatari anche i gestori di sistemi di trasporto intelligente, da intendersi, in forza dell'art. 4, par. 1 della direttiva 2010/40/CE, come «sistemi in cui sono applicate tecnologie dell'informazione e della comunicazione, nel settore del trasporto stradale, infrastrutture, veicoli e utenti compresi, e nella gestione del traffico e della mobilità nonché per interfacce con altri modi di trasporto». In capo a questi «soggetti critici», la menzionata direttiva impone obblighi volti a rafforzare la loro resilienza, quale «capacità di un soggetto critico di prevenire, attenuare, assorbire un incidente, di proteggersi da esso, di rispondervi, di resistervi, di adattarvisi e di ripristinare le proprie capacità operative».

La direttiva UE 2022/2557 non si occupa degli aspetti relativi alla cibersicurezza dei soggetti critici, dal momento che per questi ultimi valgono le disposizioni più specifiche, stabilite dalla richiamata direttiva NIS 2[44].

Maggiore impatto sulla definizione di elevati standard di *cybersecurity* ha il regolamento 2019/2144/UE, che concerne i requisiti di omologazione dei veicoli a motore e dei loro rimorchi, nonché di sistemi, componenti ed entità tecniche destinati a tali veicoli, per quanto riguarda la loro sicurezza generale e la protezione degli occupanti dei veicoli e degli altri utenti vulnerabili della strada[45].

---

[43] In base all'art. 2, par. 12 reg. cit. il prodotto TIC viene definito come «un elemento o gruppo di elementi di una rete o di un sistema informativo». Come stabilito dall'art. 2, par. 11 reg. cit. il certificato europeo di cibersicurezza è un «documento rilasciato dall'organismo pertinente che attesta che un determinato prodotto TIC, servizio TIC o processo TIC è stato oggetto di una valutazione di conformità con i requisiti di sicurezza specifici stabiliti da un sistema europeo di certificazione della cibersicurezza».

[44] V. Considerando 9.

[45] Regolamento (UE) 2019/2144 del Parlamento europeo e del Consiglio del 27 novembre 2019 relativo ai requisiti di omologazione dei veicoli a motore e dei loro rimorchi, nonché di sistemi, componenti ed entità tecniche destinati a tali veicoli, per quanto riguarda la loro sicurezza generale e la protezione degli occupanti dei veicoli e degli altri utenti vulnerabili della strada, che modifica il regolamento (UE) 2018/858 del Parlamento europeo e del Consiglio e abroga i regolamenti (CE) n. 78/2009, (CE) n.

Il regolamento sottolinea come «la connettività e l'automazione dei veicoli aumenta la possibilità di accessi a distanza non autorizzati ai dati di bordo e di modifiche illegali via etere al software»[46] e «le modifiche del software possono alterare in modo sostanziale le funzionalità dei veicoli»[47]. Esso prevede inoltre che dal 7 luglio 2024 potranno essere immatricolati e commercializzati soltanto i veicoli dotati di un c.d. «registratore di dati di evento» (RDE) o c.d. *black box* (art. 6, par. 1, lett. g reg. cit.).

La c.d. scatola nera, che serve ad acquisire maggiori informazioni sulle dinamiche di eventuali incidenti nei quali potrebbero essere coinvolti i veicoli, deve essere in grado di registrare e memorizzare in forma anonimizzata, per il periodo immediatamente antecedente, concomitante e successivo ad una collisione, i dati relativi alla velocità del veicolo, alla frenata, alla posizione ed all'inclinazione del veicolo sulla strada, lo stato e la frequenza di attivazione di tutti i suoi sistemi di sicurezza, all'attivazione del freno, nonché qualsiasi altro parametro di *input* pertinente dei sistemi di bordo di sicurezza attiva e di prevenzione degli incidenti (art. 6, par. 4 lett. a), reg. cit.)[48]. Tali dati possono essere messi a disposizione delle autorità nazionali, tramite un'interfaccia standardizzata, in base alla legislazione nazionale o europea, soltanto ai fini della ricerca e dell'analisi del sinistro.

Per evitare che i dati memorizzati nella *black box* possano essere manipolati (ad es. da parte del conducente del veicolo per evitare di incorrere in sanzioni a seguito di un incidente stradale da lui causato), i produttori dei veicoli hanno

79/2009 e (CE) n. 661/2009 del Parlamento europeo e del Consiglio e i regolamenti (CE) n. 631/2009, (UE) n. 406/2010, (UE) n. 672/2010, (UE) n. 1003/2010,(UE) n. 1005/2010, (UE) n. 1008/2010, (UE) n. 1009/2010, (UE) n. 19/2011,(UE) n. 109/2011, (UE) n. 458/2011, (UE) n. 65/2012, (UE) n. 130/2012,(UE) n. 347/2012, (UE) n. 351/2012, (UE) n. 1230/2012 e (UE) 2015/166 della Commissione.

[46] Considerando 26 reg. 2019/2144.

[47] Considerando 27 reg. 2019/2144.

[48] Viene altresì previsto, nel Considerando 14, che i dati personali relativi al conducente, trattati dal registratore di dati di evento e relativi al suo stato attenzione e la stanchezza o sul riconoscimento della distrazione, debbano essere effettuati in conformità del diritto dell'Unione sulla protezione dei dati, in particolare del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio.

l'obbligo di garantire un elevato livello di protezione e di accuratezza nella produzione dell'EDR[49].

Occorre, infine, richiamare, in questa sede, il regolamento europeo 2023/988, relativo alla sicurezza generale dei prodotti, che è entrato in vigore il 31 dicembre 2024 ed il quale persegue l'obiettivo di assicurare un elevato livello di protezione dei consumatori (art. 1). Pur non occupandosi in senso stretto di cibersicurezza dei veicoli, esso contribuisce, in via indiretta, a garantirne una maggiore protezione.

A differenza di quanto previsto dalla abrogata direttiva 2001/95/EC, il citato regolamento stabilisce che, nel valutare la sicurezza di un prodotto e, dunque, anche di un veicolo, si debbano prendere in considerazione adeguate caratteristiche di cibersicurezza «necessarie per proteggere il prodotto da influenze esterne, compresi terzi malintenzionati, se tale influenza potrebbe avere un impatto sulla sicurezza del prodotto, compresa la possibile perdita di interconnessione» (art. 6 par. 1 lett. g).

In base all'art. 9 reg. cit., all'atto dell'immissione dei prodotti sul mercato, i produttori garantiscono che essi siano stati progettati e fabbricati conformemente all'obbligo generale di sicurezza, stabilito dall'articolo 5 reg. cit.

L'OEM che ritenga o abbia motivo di credere, sulla base delle informazioni in suo possesso, che un prodotto che ha immesso sul mercato sia pericoloso dovrà adottare immediatamente le misure correttive necessarie per rendere in modo efficace il prodotto conforme, compreso il suo ritiro o il richiamo dal mercato ed informare tempestivamente i consumatori, nonché le autorità nazionali di vigilanza del mercato (art. 9, par. 8). Rilevanti sono le conseguenze anche nell'ambito del settore dei trasporti.

Qualora emerga che un nuovo veicolo, a causa delle sue vulnerabilità agli attacchi informatici, non sia sicuro e possa costituire un pericolo per i

[49] Sull'utilizzo dei dati memorizzati nell'EDR per fini investigativi v. KURACHI-KATAYAMA-SASAKI-SAITO-AJOKA, *Evaluation of Automotive Event Data Recorder towards Digital Forensics*, in *EEE Access*, 2023, 11, 81623; MARTINESCO NETTO-MIRANDA NETO-ETGENS, *A Note on Accidents Involving Autonomous Vehicles: Interdependence of Event Data Recorder, Human-Vehicle Cooperation and Legal Aspects*, in *IFAC PapersOnLine*, 2019, 51(34), 407 ss.

consumatori, si dovrà impedire che esso venga immesso sul mercato. Laddove quest'ultimo sia già in circolazione, dovrà esserne immediatamente ordinato il richiamo, vale a dire la restituzione al produttore, affinché adotti le necessarie misure per renderlo sicuro.

4.3. *Gli standard SAE sulla* cybersecurity *dei veicoli*. Il settore dell'*automotive* è caratterizzato da molteplici standard, definiti da autorevoli organizzazioni internazionali, quali, ad es., l'ISO (*International Organization for Standardization*), la SAE (*Society of Automotive Engineers*) e l'ITU (*International Telecommunication Union*).
La prima importante guida sulla sicurezza dei sistemi dei veicoli *cyber*-fisici, pubblicata dalla SAE nel 2016, è stata aggiornata nel 2021[50].
Sempre nel 2021, la SAE, in collaborazione con l'*International Standardization Organization* (ISO), ha adottato un nuovo standard ISO/SAE 21434, il quale prevede specifiche misure e procedimenti per implementare, in un'ottica di *security by-design*, la *cybersecurity* nel settore dei trasporti su strada[51]. Il menzionato standard si applica ai sistemi elettrici ed elettronici (E/E), ai componenti *hardware* e *software* ed alle interfacce dei veicoli stradali per tutto il loro ciclo di vita. Pur non prescrivendo alcun requisito tecnico in relazione alla sicurezza informatica, lo standard ISO/SAE 21434 stabilisce i requisiti per la valutazione e la gestione dei rischi cibernetici.
Affinché un veicolo possa funzionare in modo corretto e sicuro, occorre garantire il costante aggiornamento dei *software* di cui è composto. Per assicurare che i suddetti programmi informatici vengano prontamente aggiornati, nel 2023 è stato rilasciato lo standard ISO/SAE 24089, che, per la prima volta nel settore dell'industria automobilistica, prevede l'adozione di un sistema di gestione degli aggiornamenti del *software*. Si tratta, nello specifico, di un approccio unitario per la gestione dell'aggiornamento, da remoto, dei

[50] SAE, *Cybersecurity Guidebook for Cyber-Physical Vehicle Systems*, J3061_201601.
[51] ISO/SAE 21434: 2021 "*Road Vehicles - Cybersecurity Engineering*". Per un'analisi critica del menzionato standard v., in dottrina, MACHER-SCHMITTNER-VELEDAR-BRENNER, *ISO/SAE DIS 21434 Automotive Cybersecurity Standard – In a Nutshell*, in *Computer Safety, Reliability, and Security*, a cura di Casimiro-Ortmeier-Bitsch-Ferreira, 2020, 123 ss.

software di cui sono composti i moderni veicoli: i requisiti da esso stabiliti, da adottarsi da parte dei soggetti che intervengono a vario titolo nella *supply chain*, si estendono a tutti i componenti elettronici ed informatici dei veicoli.
Con la raccomandazione sulle minacce per la sicurezza dei veicoli connessi, l'ITU ha di recente definito un articolato quadro di linee guida, regole e procedure per la condivisione di informazioni che possono aiutare le OMS ad identificare, valutare, monitorare e rispondere ai rischi per i suddetti veicoli e contribuire, al contempo, a ridurre il potenziale impatto negativo dei *cyber*-attacchi sui CV[52].
Il rispetto dei menzionati standard internazionali, che non sono di per sé vincolanti, consente alle case automobilistiche di ridurre al minimo i rischi per le persone e per la sicurezza stradale, ma anche di assicurare (ed essere in grado di dimostrare) che i loro veicoli sono sicuri.
L'implementazione di tali standard contribuisce altresì ad evitare, da un lato, costosi richiami dal mercato per i veicoli che non rispettino gli standard di (*cyber*)sicurezza, e, dall'altro, significativi danni reputazionali e di immagine, legati ai deficit di sicurezza delle automobili immesse sulle strade pubbliche.

5. *I profili penali delle minacce alla* automotive cybersecurity. L'incessante sviluppo tecnologico che connota il settore automobilistico, se, da un lato, contribuisce a rendere i moderni veicoli sempre più sicuri, dall'altro, favorisce l'aumento dei rischi *cyber*[53].
Le *smart cars*, come si è visto (v. *supra*, par. 1), si configurano come complessi sistemi *cyber*-fisici, composti da parti *hardware* e *software* ed il cui corretto funzionamento dipende dalla raccolta e dal trattamento, mediante sofisticati dispositivi elettronici e sistemi informatici, di una mole molto elevata di dati (sullo stato e sulla posizione del veicolo, sui comportamenti del conducente, concernenti carte di credito e debito utilizzate, ecc.). Tali dati, che vengono raccolti ed elaborati grazie all'impiego di algoritmi, agenti artificiali e sistemi informatici, sono potenzialmente a rischio di attacchi non autorizzati posti in

[52] Recommendation ITU-T X.1371 (2020), *Security threats to connected vehicles*.
[53] MEYER-ELVIK-JOHNSSON, *Risk Analysis*, cit., 227 ss.

essere da soggetti malintenzionati (per finalità economiche, per vendetta, ecc.)[54].

I *cyber*-rischi riguardano non solo le auto connesse o autonome (c.d. *self driving cars*), ma anche i veicoli con un limitato livello di automazione[55]. Si tratta in particolare di minacce che, in un prossimo futuro, potrebbero essere più insidiose rispetto a quelle che attualmente hanno ad oggetto i sistemi informatici privati (frodi, danneggiamenti informatici, intercettazioni di dati, ecc.). Gli attacchi ai veicoli intelligenti potrebbero invero avere conseguenze negative non solo per i conducenti ed i passeggeri da essi trasportati, ma anche per i pedoni ed i terzi coinvolti nella circolazione stradale e, più in generale, per la sicurezza dei trasporti[56].

Gli attacchi cibernetici nel settore dell'*automotive*, a seconda della loro gravità, possono ostacolare la funzionalità di alcune operazioni del veicolo intelligente, comprometterne la sicurezza, alternarne le prestazioni mediante modifiche alla parte *software* ovvero incidere sulla riservatezza, sulla integrità e disponibilità dei dati informatici trattati dal veicolo[57].

Prevedere le tipologie di *cyber*-attacchi ai quali potrebbero essere sottoposte, in un prossimo futuro, le *smart cars* è alquanto complesso. Il loro effettivo impiego nella circolazione stradale non ha, infatti, raggiunto livelli significativi e le "aggressioni" nei loro confronti sono ancora limitate[58].

---

[54] SIDDIQUI-KHAN-SEZER-EYER, *Bird's-eye View in The Automotive Cybersecurity Landscape & Challenges in adopting AI/ML*, in *2021 Sixth International Conference on Fog and Mobile Edge Computing,* a cura di Abdennadhr-Benkhelifa-Lloret-Jararweh, 2021, 1 ss., consultabile al sito *www.doi.org/10.1109/FMEC54266.2021.9732568.*

[55] WIMERSKIRSCH, *Dominic Derrick Dominic, Assessing Risk: Identifying and Analyzing Cybersecurity Threats to Automated Vehicles*, University of Michigan, 2018, consultabile al sito *www.mcity.umich.edu/wp-content/uploads/2017/12/Mcity-whitepaper_cybersecurity.pdf.*

[56] Rispetto ad alcune *smart cars* il proprietario può oggi già avviare, mediante una apposita *app*, il motore da remoto (ad es. per riscaldare o raffreddare l'abitacolo ad una temperatura confortevole); quest'ultimo, però, non è collegato in senso stretto alla rete. Non è pertanto (ancora) possibile, rispetto ai veicoli intelligenti attualmente in commercio, guidarli da remoto o prenderne il pieno controllo attraverso reti *wireless* o il *web* (ad es. al fine di utilizzarli quali strumenti letali da far schiantare contro pedoni, ecc.).

[57] La tabella A1, allegato 5 reg. n. 155 UNECE richiama, tra le principali minacce cibernetiche ai veicoli *smart*, quelle che riguardano: i *server* di *back-end* connessi ai veicoli in circolazione; i canali di comunicazione e le loro procedure di aggiornamento; azioni umane non intenzionali che facilitino un attacco informatico; la connettività ed i collegamenti esterni ed i dati informatici; potenziali vulnerabilità che potrebbero essere sfruttate da soggetti malintenzionati, se non sufficientemente risolte.

[58] Cfr. MEYER-ELVIK, JOHNSSON, *Risk Analysis*, cit., 227 ss.

Il continuo e rapido sviluppo delle nuove tecnologie, in specie dell'IA, che vengono impiegate nel settore dell'*automotive* contribuisce inoltre a rendere incerta ogni valutazione in merito al grado di resilienza delle *smart cars* alle future minacce cibernetiche. Onde evitare pertanto che l'analisi dei rischi in questo ambito si trasformi in un mero esercizio speculativo, pare più corretto prendere in considerazione, in questa sede, soltanto le vulnerabilità rispetto alle quali sussistano già oggettive evidenze.

Attualmente le principali *cyber*-minacce nel settore *automotive* concernono: 1) le reti *network* ed i canali di comunicazione dei veicoli; 2) la componente *software* e *hardware* dei veicoli; 3) le radiofrequenze periferiche[59]. Questi attacchi possono portare alla indebita "appropriazione" di dati informatici (personali, sensibili, relativi a sistemi di pagamento, ecc.), all'installazione di *malware* e *spyware*, al danneggiamento di dati, alla compromissione ovvero all'alterazione delle funzionalità di un veicolo[60].

5.1. *Gli attacchi alle reti di comunicazione.* Recenti *report* ed esperimenti condotti da gruppi di ricerca e c.d. *ethical hackers* hanno dimostrato come i dispositivi ed i sistemi informatici di cui sono dotati i moderni veicoli intelligenti, ed in specie le reti mobili e *wireless*, da cui dipende il funzionamento dei sistemi di *infotainment* e l'aggiornamento di molte loro funzionalità, siano particolarmente vulnerabili agli attacchi cibernetici[61].

---

[59] In base ad una recente analisi degli incidenti cibernetici nel settore automobilistico, verificatisi tra il 2020 ed il 2021, l'89.3% degli attacchi avrebbe avuto ad oggetto i canali di comunicazione dei veicoli; l'87.7% i dati informatici; il 47.1% le connessioni con reti esterne (Upstream, *Global Automotive Cybersecurity Report*, 2023). Sulle principali tipologie di attacchi v. anche il recente *report* di IOActive, elaborato da BEAMOUNT, *Commonalities in Vehicle Vulnerabilities*, 2023, 1 ss., 22 s., consultabile al sito *www.ioactive.com/ioactive-commonalities-vehicle-vulnerabilities-22update/*. Pur includendo la tipologia degli attacchi alla parte c.d. *hardware*, l'A. evidenzia come questi ultimi siano sempre più ridotti, dal momento che presuppongono il contatto fisico del soggetto malintenzionato con il veicolo. Si pensi, a titolo esemplificativo, al soggetto che inserisca una USB "infetta" nel sistema di *infotainment* di un veicolo per accedere all'area di controllo (*controlled area network* o CAN).

[60] Cfr. Kasperky Ics Cert, *Cybersecurity*, cit., 1 ss.

[61] Cfr. Upstream, *Global Automotive Cybersecurity Report*, 2024, in base al quale gli accessi abusivi alle *smart cars* costituirebbero oltre l'85% degli attacchi cibernetici nel settore *automotive*. Parte degli attacchi cibernetici commessi a danno di CAV si realizzano anche attraverso lo sfruttamento delle vulnerabilità delle *app* degli *smartphone* e dei *cloud servers*.

Mediante il c.d. *automotive hacking* è possibile ottenere un accesso non autorizzato ai sistemi informatici di cui sono dotate le *smart cars*, per procurarsi illecitamente i dati memorizzati e trattati al loro interno, per alterarli o danneggiarli[62]. Tale fenomeno criminoso mette innanzitutto in pericolo la riservatezza dei dati contenuti nei c.d. *in-vehicle systems*. Esso può inoltre costituire una seria minaccia per l'integrità e la disponibilità delle apparecchiature informatiche e telematiche da cui dipende il corretto funzionamento del veicolo e, di conseguenza, anche per la vita del conducente, dei passeggeri e di tutti coloro che sono coinvolti nella circolazione stradale. Paradigmatici, in tal senso, sono gli accessi non autorizzati ai sistemi di *infotainment* (*in-vehicle-infotainment system*: di seguito IVI)[63].

I proprietari delle *smart cars*, mediante apposite *app*, possono collegare il loro cellulare ai moderni sistemi IVI, i quali sono a loro volta connessi a *network*, reti *wireless* e mobili (4G, 5 G) ed a internet[64]. Vi è così la possibilità di interagire, anche da remoto, con il proprio veicolo, gestire numerose informazioni private e sensibili (la geolocalizzazione, la destinazione, le chiamate, la rubrica del telefono, dati di carte di credito, ecc.), ottenere aggiornamenti *over-the-air*, ecc.[65]. Soggetti malintenzionati potrebbero, di

[62] WENZELF, *Not Even Remotely Liable: Smart Car Hacking Liability*, in *U. Ill. J.L. Tech. & Pol'y*, 2017, 49 ss.; GREEN, *The Self Drive Act: An Opportunity to Re-Legislative a Minimum Cybersecurity Federal Framework for Autonomous Vehicles*, in *Santa Clara Law Review*, 2020, 60, 217 ss., 228 ss.; più di recente Upstream, *Global Automotive Cybersecurity Report*, 2024, cit., 40.

[63] Per un'analisi delle principali modalità di attacco agli IVI v., ad es., COSTANTINO-DE VINCENZI-MATTEUCCI, *A Vehicle Firmware Security Vulnerability: an IVI Exploitation,* in *Journal of Computer Virology and Hacking Techniques*, 20, 2024, 681 ss.

[64] Per venire incontro alle richieste dei consumatori, le case produttrici stanno dotando le moderne *smart cars* di applicazioni per consentirne l'interazione mediante dispositivi mobili. I proprietari dei c.d. *computer-on-wheels* possono così controllare, attraverso il loro *smartphone*, molteplici funzioni (apertura dell'auto, accensione del motore, del riscaldamento, ecc.) ed ottenere numerose informazioni (sullo stato dei pneumatici, dei sensori, sul livello di carburante, ecc.). Sfruttando le vulnerabilità presenti nelle menzionate app e nell'interfaccia di programmazione delle applicazioni (API), i soggetti malintenzionati possono ottenere l'accesso ad alcuni sistemi informatici di cui sono dotati i veicoli intelligenti ed in questo modo alterare alcuni dati, disattivare i sistemi di allarme, ecc.

[65] Sicuramente all'avanguardia, in tal senso, è l'IVI *system* installato sulla Tesla Model 3, che consente al proprietario di regolare la sospensione, selezionare il profilo di guida, attivare alcune funzionalità di assistenza alla guida. Il sistema permette inoltre di accedere a numerose informazioni sullo stato del veicolo (autonomia della batteria, pressione degli pneumatici, consumo energetico, ecc.).

conseguenza, intercettare i canali di comunicazione (VANATs), manipolare e sottrarre informazioni per fini illeciti, ecc.[66].

Un paradigmatico esempio di *automotive hacking* si verificò nel 2015 ai danni del sistema IVI della Jeep della Chrysler[67]. Due ricercatori, sfruttando le vulnerabilità in un protocollo di trasmissione di dati, riuscirono ad accedere, da remoto, a vari servizi di *infotainment*, nonché al GPS, al condizionatore (HVAC), alla radio e ai *display* installati sul veicolo[68]. La casa automobilistica americana fu così costretta a ritirare dal commercio oltre un milione di veicoli.

Nonostante gli sforzi fatti negli ultimi anni da parte dei costruttori di veicoli *smart* per innalzare i livelli di sicurezza, i sistemi di *infotainment* presentano ancora alcune vulnerabilità e, per questo motivo, sono a rischio di attacchi.

Non pare, invece, realistico, ad oggi, che un *hacker*, sfruttando le "falle" nella sicurezza del c.d. *Internet of Vehicles* (IoV) possa riuscire, da remoto, ad accedere abusivamente ad un CAV ed intervenire sulle principali funzionalità di guida o prendere il controllo di altri veicoli interconnessi (mediante reti V2V mediante *wireless*, reti mobili, IoV, ecc.).

Le condotte di *hacking* ai danni dei dispositivi e dei sistemi informatici che compongono le *smart cars* non sollevano, sul piano penale, particolari problemi applicativi. Esse possono essere pacificamente sussunte nel delitto di accesso abusivo ad un sistema informatico o telematico protetto da misure di sicurezza di cui all'art. 615-*ter* c.p.[69].

---

[66] TAEIHAGH-MIN LIM, *Governing Autonomous Vehicles: Emerging Responses for Safety, Liability, Privacy, Cybersecurity, and Industry Risks*, in *Transport Review*, 2019, 39, 103 ss.

[67] SCHELLEKENS, *Car Hacking: Navigating The Regulatory Landscape*, in *Computer Law and Security Review*, 32, 2016, 307 ss.

[68] V. JEONG-KANG-RYU-KIM, *Infotainment System Matters: Understanding the Impact and Implications of In-Vehicle Infotainment System Hacking with Automotive Grade Linux*, in Codaspy '23, *Proceedings of the Thirteenth ACM Conference on Data and Application Security and Privacy*, 2023, 201 ss.

[69] SALVADORI, *Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale*, in *Riv. it. dir. proc. pen.*, 2021, 83 ss., 112; più in generale, sulla controversa formulazione dell'art. 615-*ter* c.p. sia consentito rinviare a ID., *Il delitto di accesso abusivo ad un sistema informatico o telematico. Sono maturi i tempi per un suo restyling?*, in AA.VV., *La riforma dei reati contro la persona. Proposte dei gruppi di lavoro dell'AIPDP*, 2023, 579 ss., consultabile al sito *www.aipdp.it/allegato_prodotti/225_AIPDP-DIPLAP_Riforma_reati_contro_la_persona_a_cura_di_AIPDP-DIPLAP.pdf*.

Il concetto di sistema informatico, nell'assenza di una definizione legale espressa, viene pacificamente inteso, in linea con quanto stabilito dall'art. 2, lett. a) direttiva 2013/40/UE, come «un'apparecchiatura o gruppo di apparecchiature interconnesse o collegate, uno o più dei quali svolge un trattamento automatico di dati informatici secondo un programma»[70]. Si tratta, dunque, di un dispositivo composto da parti *hardware* e *software*, che consente il processamento automatico di dati informatici[71]. Ed in tal senso, non vi sono dubbi che i moderni veicoli intelligenti siano composti da sistemi informatici.
Con l'art. 16, co. 1, lett. b) L. n. 90/2024 è stato esteso l'ambito di applicazione della circostanza aggravante di cui all'art. 615-*ter*, co. 2, n. 3 c.p. Essa prevede un aumento di pena (reclusione da 2 a 10 anni, in luogo della reclusione fino a tre anni prevista per il fatto-base di cui al co. 1 dell'art. cit.), qualora al fatto illecito di accesso abusivo consegua la distruzione, il danneggiamento ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al titolare del sistema o l'interruzione, in tutto o in parte, del funzionamento del sistema informatico ovvero la distruzione o il danneggiamento dei dati e dei programmi informatici in esso contenuti. Tale previsione potrebbe applicarsi, ad esempio, nei casi, tutt'altro che infrequenti, in cui un *hacker*, a seguito dell'intrusione non consentita nei sistemi di *infotainment* di una *smart car*, danneggi i dati contenuti all'interno del sistema di bordo. Trattandosi, tuttavia, di una previsione che si configura come un c.d. reato aggravato dall'evento, il risultato qualificante ed aggravatore del danneggiamento richiede, sul piano soggettivo, la mera colpa[72]. Qualora, infatti, il danneggiamento fosse voluto dal soggetto agente l'ipotesi aggravata di accesso abusivo di cui all'art. 615-*ter*, co 2, lett. b. c.p. verrebbe a concorrere con i delitti (dolosi) di danneggiamento di dati o di sistemi informatici.

---

[70] Sostanzialmente identica è la definizione contenuta all'art. 1, lett. a) *Cybercrime Convention* del 2001 del Consiglio d'Europa.
[71] Cfr. Council of Europe, *Cybercrime Convention*, Explanatory report, par. 23. *Contra* LANZI, *Self-driving cars*, cit., 107, il quale ritiene che il concetto normativo di sistema informatico abbracci soltanto la parte *hardware* e non anche quella *software*.
[72] SALVADORI, *I reati*, cit., 725. È, dunque, criticabile la scelta operata dal legislatore del 2024 che, tra gli eventi aggravatori, ha incluso anche l'ipotesi di sottrazione, anche mediante riproduzione o trasmissione, di dati, rispetto alla quale pare più coerente la sussistenza del dolo, in luogo della colpa.

In base all'art. 615-*ter*, co. 3 c.p., novellato dall'art. 16 L. n. 90/2024, è previsto un significativo aumento di pena (rispettivamente da tre a dieci anni e da quattro a dodici anni) qualora l'ipotesi-base di accesso abusivo ad un sistema informatico o telematico di cui al co. 1 dell'art. 615-*ter* c.p. ovvero le ipotesi circostanziate di cui al co. 2 del menzionato articolo abbiano ad oggetto sistemi informatici o telematici «di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile» o, comunque, «di interesse pubblico». La suddetta circostanza aggravante ad effetto speciale potrebbe applicarsi, qualora il soggetto agente riesca ad accedere *invito domino* al sistema informatico di un veicolo intelligente, che effettui un servizio di trasporto pubblico (ad es. un robotaxi).

I c.d. *hacking tools* che vengono impiegati dai criminali per accedere abusivamente ai sistemi informatici di cui sono dotate le *smart cars* si trovano spesso *online* ed in specie sul *dark web*[73]. Il fatto di mettere a disposizione sul *web* o, comunque, di diffondere, consegnare o anche soltanto detenere questi *malware*, qualora venga posto in essere al fine di trarne un profitto o di arrecare un danno a terzi, potrà essere sussunto nell'alveo dell'art. 615-*quater* c.p.[74]

La menzionata disposizione, anticipando ulteriormente la tutela penale della riservatezza e della sicurezza dei sistemi, consente di punire anche chi si limiti a fornire (ad es. nell'ambito di un gruppo Telegram o di una *community* di *hacker* sulla darknet) indicazioni o istruzioni idonee a raggiungere i predetti scopi[75].

5.2. *I danneggiamenti alla parte software e hardware.* Soggetti malintenzionati possono sfruttare le vulnerabilità dei complessi ecosistemi *software* di cui sono

[73] Cfr. Upstream, *Global Automotive Cybersecurity Report*, 2023, 70 ss.

[74] Sulle modifiche apportate all'art. 615-*quater* c.p. dall'art. 19, co. 1, lett. c) L. 23 dicembre 2021, n. 238 v. CRESCIOLI, *Le recenti modifiche ai reati cibernetici, tra tardivo recepimento delle direttive europee e nuove incriminazioni: riflessioni critiche*, in *Arch. pen. web*, 2021, 2, 1 ss.; volendo v. anche SALVADORI, *I reati contro la riservatezza informatica*, in *Cybercrime*[2], a cura di Cadoppi-Canestrari-Manna-Papa, Milano, 2023, 729 ss.

[75] Sulla peculiare struttura del menzionato reato sia consentito rinviare a SALVADORI, *Criminalità informatica e tecniche di anticipazione della tutela penale. L'incriminazione dei "*dual-use software*"*, in *Riv. it. dir. proc. pen.*, 2017, 2, 568 ss., 747 ss., 759 ss.; ID., *I reati contro la riservatezza informatica*, cit., 729 ss.

dotati i moderni veicoli intelligenti per finalità illecite. Si pensi, a titolo paradigmatico, agli attacchi ai sistemi operativi, alle ECU, alle alterazioni o manipolazioni di dati, programmi informatici o al sistema di *infotainment* mediante *malware* o l'impedimento del loro corretto funzionamento cagionato da un programma *ransomware*.

A tutela della parte *software* dei moderni veicoli *cyber*-fisici potranno applicarsi, laddove ne sussistano tutti gli elementi tipici (oggettivi e soggettivi), i reati cibernetici, il cui oggetto materiale è costituito da dati ovvero sistemi informatici. Ne consegue che gli attacchi alle componenti *software,* laddove determinino l'alterazione, il danneggiamento o la distruzione non autorizzata di dati o programmi informatici potranno essere pacificamente ricondotti ai delitti di danneggiamento di dati informatici (privati o pubblici) di cui agli artt. 635-*bis* ss. c.p.[76].

Qualora, mediante i menzionati fatti di danneggiamento, si cagioni l'inservibilità, totale o parziale, del sistema informatico da cui dipende il funzionamento di una *smart car* o si ostacoli gravemente il suo funzionamento si potranno applicare i più gravi reati di danneggiamento di sistemi informatici (privati o pubblici) di cui agli artt. 635-*ter* e 635-*quater* c.p.[77].

Penalmente rilevante sarà altresì la condotta del criminale informatico che, fuori dai casi consentiti dalla legge, installi o faccia uso di uno *spyware* per intercettare fraudolentemente le comunicazioni informatiche, che intercorrono, ad esempio, tra la CAN *bus* ed i diversi componenti informatici del veicolo, tra il suo sistema di *infotainment* e le reti a cui è connesso ovvero tra il veicolo e lo *smartphone* del suo proprietario che mediante quest'ultimo potrebbe attivare determinate funzionalità del mezzo. Suddette condotte potranno essere ricondotte alle fattispecie che puniscono le intercettazioni non

[76] Cfr. SALVADORI, *I danneggiamenti informatici*, in *Diritto penale dell'informatica*, a cura di Parodi-Sellaroli, Milano, 2000, 597 ss., 607 ss.; CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici*, in *Cybercrime*, cit., 810 ss., in specie 847 ss.

[77] SALVADORI, *I danneggiamenti informatici*, cit., 597 ss.; CAPPELLINI, *I delitti contro l'integrità dei dati,* cit., 847 ss.

autorizzate di dati informatici (artt. 617-*quater*, 617-*quinquies*, 617-*sexies* c.p.)[78].

5.3. *Le interferenze nelle radiofrequenze.* Le nuove tecnologie, applicate al settore dei trasporti, contribuiscono a sviluppare nuovi meccanismi per impedire, da un lato, il furto di veicoli e, dall'altro, per rendere più semplici determinate funzioni (accensione e spegnimento da remoto del motore, del riscaldamento e dell'aria condizionata, ecc.). In questa ottica, si inseriscono i moderni veicoli dotati di sistemi di accesso senza chiavi[79].

Portachiavi intelligenti, muniti di un trasmettitore di onde, o semplici *smartphone* emettono segnali radio nel raggio di alcuni metri, che vengono riconosciuti dal veicolo ad essi associato. Il proprietario del veicolo mediante questi dispositivi può facilmente aprire o chiudere l'auto a distanza. Queste tecnologie possono, però, essere sfruttate anche da soggetti malintenzionati per introdursi illecitamente nel veicolo e sottrarlo, senza necessità di disporre delle chiavi.

Uno dei principali metodi impiegati per sottrarre le auto intelligenti consiste nella realizzazione di un c.d. *relay attack*[80]. I criminali possono facilmente intercettare le comunicazioni tra i portachiavi intelligenti ed il veicolo *smart* mediante l'impiego fraudolento di un trasmettitore o di un dispositivo per la riproduzione di segnali radio, collocato in prossimità del veicolo, riuscendo ad aprirlo e ad avviare il motore. Essi possono intercettare anche il segnale di un portachiavi intelligente che si trovi all'interno del domicilio del proprietario del veicolo. Una volta riprodotto il segnale dei comandi, è possibile aprire, senza disporre della chiave, il veicolo e, nelle *smart cars* più moderne, avviare anche il motore.

---

[78] Con la L. n. 90/2024 il Parlamento, oltre ad aver inasprito il trattamento sanzionatorio per le fattispecie di intercettazione di dati informatici, ha provveduto a modificarne in parte la formulazione. Sul punto v. SALVADORI, *Art. 24-bis*, in *Compliance, Responsabilità da reato degli enti collettivi*, a cura di Castronuovo-De Simone-Ginevra-Lionzo-Negri-Varraso, Milano, 2024, 534 ss.

[79] Sulle modalità di commissione dei c.d. *remote keyless entry systems* v. Upstream, *Global Automotive Cybersecurity*, 2024, cit., 56.

[80] Upstream, H12023, *Automotive Cyber Trend Report*, cit., 13; ed in specie Upstream, *Global Automotive Cybersecurity*, 2024, cit., 57 ss.

L'aumento dei furti d'auto mediante *relay attacks* è facilitato anche dal fatto che *online*, ed in specie sulla *darknet*, sono sempre più frequenti i siti illegali che forniscono informazioni dettagliate e *tutorials* su come realizzare tali attacchi, sugli strumenti da utilizzare, ecc.[81]

Le frequenze radio che vengono trasmesse da un c.d. *key fob* al veicolo non sono comunicazioni informatiche o telematiche riservate, bensì meri segnali elettromagnetici. Per questo motivo le intercettazioni dei segnali radio, poste in essere nell'ambito degli attacchi di tipo *relay*, non sono sussumibili nei reati di intercettazione informatiche di cui agli artt. 617-*quinquies* c.p. Va detto, tuttavia, che, per effetto della disposizione di cui all'art. 623-*bis* c.p., la tutela penale prevista per le comunicazioni informatiche e telematiche si estende a «*qualunque altra trasmissione a distanza di suoni, immagini o altri dati*».

Qualora il *relay attack* vada a buon fine ed il malintenzionato riesca a impossessarsi del veicolo altrui si configurerà un comune reato di furto di cui all'art. 624 c.p. In questi casi si potrà inoltre applicare la circostanza aggravante di cui all'art. 625, co. 1, n. 1 c.p., dal momento il ricorso ad un *relay attack* potrebbe essere equiparato all'utilizzo di mezzi fraudolenti. Si tratta invero di ipotesi in cui il soggetto agente ricorre a mezzi insidiosi idonei ad eludere le cautele poste in essere dal proprietario del veicolo.

La menzionata circostanza aggravante sarebbe inoltre compatibile con quella relativa all'impossessamento di cose esposte a pubblica fede di cui all'art. cit.

6. Cyber-*attacchi e tutela penale della sicurezza dei trasporti.* A fronte dell'aumento dei rischi cibernetici per il settore dell'*automotive* e dei conseguenti pericoli che potrebbero derivare per fondamentali beni giuridici individuali (patrimonio, integrità fisica, vita) e collettivi (sicurezza stradale, incolumità pubblica), un settore della dottrina si è posto la questione della (eventuale) necessità di introdurre nuove norme incriminatrici a tutela della sicurezza dei trasporti[82].

---

[81] Upstream, *Global Automotive Cybersecurity*, 2024, cit., 30.

[82] A favore dell'introduzione di nuove norme incriminatrici v., nella dottrina americana, GLANCY, *Autonomous and Automated and Connected Cars Oh My! First Generation Autonomous Cars in the Legal Ecosystem*, in *Minnesota Journal of Law, Science, and Technology*, 2015, 16, 619 ss., 663 s.;

Ritenendo che la vigente normativa penale di contrasto al *cybercrime* non sia in grado di tutelare adeguatamente la *automotive cybersecurity*, è stata proposta, di recente, l'introduzione di un reato *ad hoc* per punire «l'abusiva alterazione di sistemi di guida autonoma»[83]. Secondo tale orientamento, la nuova norma incriminatrice, in linea con quanto stabilito dal delitto di attentato alla sicurezza dei trasporti di cui all'art. 432 c.p., dovrebbe punire «quei soli fatti connaturati da una effettiva messa in pericolo della sicurezza stradale, e quindi che riguardino le funzioni fondamentali di guida (frenata, accelerata, ecc.), così come la capacità del veicolo di orientarsi e di "interagire" nello spazio circostante, e quindi individuare e scansare altri veicoli o ostacoli sul sedime stradale»[84].

Il prospettato inserimento di questa nuova norma incriminatrice, che si intenderebbe collocare all'interno del codice della strada, si giustificherebbe, secondo tale orientamento, per la (presunta) assenza nel nostro ordinamento di adeguate fattispecie in grado di punire le più insidiose attività di *hackeraggio* di una *smart car*, che sono tali da compromettere il corretto funzionamento e, quindi, la sicurezza del sistema (informatico) di guida del medesimo, costituendo un rilevante pericolo per l'incolumità pubblica[85]. Questa tesi non pare, però, persuasiva.

L'abusiva alterazione o manipolazione dei dati informatici e dei programmi informatici che integrano la parte *software* di una *smart car*, così come ogni comportamento che renda inservibili i sistemi informatici o telematici di cui sono dotate o che ne ostacoli gravemente il funzionamento hanno già rilievo penale nel nostro ordinamento. Si tratta, infatti, di eventi lesivi riconducibili al c.d. microsistema normativo dei danneggiamenti informatici (artt. 635-*bis* ss. c.p.)[86].

PALODICHUK, *Driving into the Digital Age: How SDVs Will Change the Law and Its Enforcement*, in *Minnesota Journal of Law, Science, and Technology*, 2015, 16, 827 ss., 831.

[83] LANZI, *Self-driving cars*, cit., 109 ss.

[84] LANZI, *Self-driving cars*, cit., 110.

[85] *Ibid.*

[86] V. *supra*, par. 5.2.

Si è giustamente evidenziato come gli attacchi cibernetici nei confronti delle auto intelligenti interconnesse, oltre ad offendere i beni giuridici della integrità e della disponibilità dei dati e dei sistemi informatici che le compongono, potrebbero al contempo mettere in pericolo la sicurezza dei trasporti, quale bene strumentale o prodromico alla tutela dell'incolumità pubblica[87]. Ma nel titolo VI del libro secondo del Codice penale già esiste un delitto volto a punire «attentati alla sicurezza dei trasporti» (art. 432 c.p.)[88]. L'introduzione di un nuovo reato, analogo quello dell'art. 432 c.p., verrebbe pertanto ad integrare una norma "fotocopia", con un effetto meramente simbolico[89].

È indubbio che la norma incriminatrice di cui all'art. 432 c.p. sconti oggi un oggettivo limite. A causa della sua anacronistica formulazione, il suo ambito di applicazione è, infatti, ridotto ai soli fatti (consumati o anche solo tentati) di danneggiamento o di distruzione dei veicoli destinati al *trasporto pubblico* su strada, e tali da esporre concretamente a pericolo la sicurezza dei trasporti[90].

La pubblica incolumità, nell'ambito dell'art. 432 c.p., è tutelata esclusivamente in relazione ai «trasporti pubblici», vale a dire «quelli di cui il pubblico può

---

[87] LANZI, *Self-driving cars*, cit., 109. Più in generale, sulle diverse nozioni di sicurezza dei trasporti e incolumità pubblica che, pure presentando oggettive diversità, presentano profili di coincidenza v. i rilievi di ARDIZZONE, voce *Naufragio, disastro aviatorio, disastro ferroviario*, in *Dig. disc. pen*, 1994, 3, 222 ss., 226.

[88] Sebbene la disposizione venga qualificata dal legislatore del 1930 in termini di «*attentato*», la dottrina maggioritaria ritiene che l'art. 432 c.p. integri, in ragione della formulazione del fatto di reato che richiama espressamente la messa in pericolo della sicurezza dei trasporti, una ipotesi di reato di pericolo concreto. In questi termini v già BETTIOL, *Considerazioni in tema di delitti di attentato*, in *Ind. pen.*, 1975, 29 ss., 38 s.; analogamente PICOTTI, *Il dolo specifico. Un'indagine sugli 'elementi finalistici' delle fattispecie penali*, Milano, 1993, 189; ed in specie GARGANI, *Il danno qualificato dal pericolo. Profili sistematici e politico-criminali dei delitti contro l'incolumità pubblica*, Torino, 2005, 303 s. Dello stesso parere Cass., Sez. I, 28 giugno 2017, n. 7203. Di diverso parere PARODI GIUSINO, *I reati di pericolo tra dogmatica e politica criminale*, Milano, 1990, 270 ss., 272, secondo il quale l'art. 432 c.p. si configurerebbe come un reato di pericolo astratto, seppur «della forma di esso più vicina al pericolo concreto».

[89] Sugli effetti distorsivi legati all'introduzione di norme incriminatrici c.d. "doppione" v. gli acuti rilievi di BONINI, *La funzione simbolica nel diritto penale del bene giuridico*, Napoli, 2018, 109 ss.

[90] Sugli oggettivi limiti dell'art. 432 c.p. v., per tutti, MORGANTE, *In tema di attentato alla sicurezza dei trasporti: limiti della disciplina attuale e prospettive di riforma*, in *Riv. it. dir. proc. pen.*, 1998, 2, 568 ss.; GARGANI, *Reati contro l'incolumità pubblica*, tomo I, *Reati di comune pericolo mediante violenza*, in *Trattato di diritto penale*, diretto da Grosso-Padovani-Pagliaro, Milano, 2008, 387 ss. Sulla peculiare struttura oggettiva e soggettiva della norma in esame v., più in generale, BATTAGLINI-BRUNO, voce *Incolumità pubblica (delitti contro la)*, in *NsDI,* 1962, vol. VIII, 542 ss., 554 ss.; GARGANI, *Il danno qualificato dal pericolo*, cit., 304 ss.

profittare direttamente, condizionatamente o incondizionatamente, siano essi esercitati dallo Stato o da altro ente pubblico ovvero da un'impresa esercente servizi pubblici o di pubblica necessità o anche da un privato concessionario o autorizzato»[91]. Ogni "attentato" ad un'auto intelligente privata, pur se tale da mettere in pericolo la sicurezza dei trasporti, non sarebbe di per sé penalmente rilevante.

L'esclusione dall'ambito di tutela dell'art. 432 c.p. dei mezzi di trasporto privati non è incentrata sulle modalità e dei luoghi di transito, essendo sostanzialmente identici a quelli dei mezzi pubblici. Essa è data piuttosto dalla fruizione di questi ultimi da parte di un numero indeterminato di persone[92]. Evidente è pertanto il contrasto della menzionata disposizione con il principio di uguaglianza, dal momento che «l'avvalersi di un mezzo di trasporto pubblico o privato è una circostanza occasionale che non giustifica diverse ipotesi di tutela se al medesimo pericolo sono esposti i medesimi beni giuridici»[93].

Vi è, dunque, una oggettiva inadeguatezza della normativa penale vigente a rispondere alle esigenze di tutela della sicurezza dei trasporti privati, che, come dimostra l'evoluzione del mercato dell'*automotive*, è sempre più *smart*.

6.1. *La rilevanza penale del c.d. dirottamento di veicoli intelligenti.* L'oggettiva lacuna legislativa, che, come sì è detto (*supra*, par. 6), non consente di punire i potenziali attacchi cibernetici alle *smart cars* private e tali da mettere in pericolo la sicurezza dei trasporti, potrebbe essere colmata, *de jure condito*, ricorrendo alla fattispecie di "disastro innominato" di cui all'art. 434 c.p. Essa punisce il compimento di fatti diretti ala realizzazione di «un altro disastro», quale figura "di chiusura" rispetto alle ipotesi speciali di disastri c.d. "nominati", contemplati all'interno del capo primo, relativo ai delitti di comune pericolo mediante violenza, del titolo VI del libro secondo del Codice penale[94].

[91] Relazione ministeriale sul progetto del Codice penale, II, 1930.
[92] MORGANTE, *In tema di attentato*, cit., 570.
[93] MORGANTE, *In tema di attentato*, cit., 569.
[94] Sulla struttura dell'art. 434 c.p., ed in specie sulla «residualità unidirezionale» della controversa ipotesi di disastro innominato v. GARGANI, *Reati contro l'incolumità pubblica*, cit., 456 ss.

La elasticità, la genericità e la vaghezza del reato di cui all'art. 434 c.p., che, nel definire il fatto tipico, impiega un'espressione normativa («altro disastro») in sé ambigua e polisensa, potrebbe, a prima vista, consentire di punire (in futuro) la realizzazione di un attacco "su larga scala" (ad es. *DoS o DDS attack*) ai sistemi informatici da cui dipende, in tutto o in parte, il corretto funzionamento di una flotta di *smart cars* private, connesse tra loro (V2V) ed alla infrastruttura stradale (V2I). Questa tipologia di attacchi potrebbero, infatti, cagionare un "macro-danneggiamento", tale da paralizzare il traffico con conseguenti rilevanti incidenti automobilistici[95]. Va ribadito, tuttavia, che, ad oggi, non vi sono ancora in circolazione autoveicoli (pubblici e privati) completamente connessi via IoV ad altri mezzi e che possano essere guidati o, comunque, controllati *in toto* da remoto e, dunque, senza la presenza fisica del guidatore a bordo.

Le ipotesi di "dirottamento informatico" di una *smart car* o, addirittura, di una flotta di veicoli intelligenti sono, allo stato attuale, irrealistiche, oltre che irrealizzabili, dato che la messa in circolazione di CAV non sarebbe, comunque, autorizzata dalla vigente normativa nazionale.

Ma anche volendo ammettere la possibilità di forme di "dirottamento" di veicoli intelligenti, al fine di potersi ritenere integrata la fattispecie di disastro innominato rispetto a ipotesi, più o meno futuribili, di c.d. *mass disaster* nel settore della *smart mobility* occorrerebbe accertare, sul piano c.d. dimensionale, la sussistenza di un «evento distruttivo di proporzioni straordinarie, anche se non necessariamente immani, atto a produrre effetti dannosi gravi, complessi ed estesi»[96]. Il menzionato evento, innescato da una

[95] Sull'originaria applicazione giurisprudenziale della fattispecie di "disastro innominato" in relazione ai gravi incidenti automobilistici v. GARGANI, *Reati contro l'incolumità pubblica*, cit., 451 s., cui si rinvia anche per alcuni riferimenti giurisprudenziali. Più in generale, sulla complessa determinazione della materialità del disastro innominato v., per tutti, ARDIZZONE, voce *Crollo di costruzioni ed altri disastri dolosi*, in *Dig. disc. pen.*, Torino, 1989, vol. III, 273 ss., 275; MARINUCCI, voce *Crollo di costruzioni*, in *Enc. dir.*, Milano, 1962, vol. XI, 410 ss.; PIERGALLINI, *Danno da prodotto e responsabilità penale. Profili dommatici e politico-criminali*, Milano, 2004, 279 ss.

[96] In questi termini, in relazione alla configurazione dell'art. 434 c.p., Corte cost., 1° agosto 2008, n. 327, con nota di GIUNTA, *I contorni del «disastro innominato» e l'ombra del «disastro ambientale» alla luce del principio di determinatezza*, in *Giur. cost.*, 2008, 3539 ss.

condotta violenta, dovrebbe provocare, sul piano della proiezione offensiva, un effettivo pericolo per la vita o per l'integrità fisica di una pluralità di persone[97].

7. *Considerazioni finali.* Negli ultimi anni, gli organismi sovranazionali (ed in specie l'UNECE e la UE) hanno fatto notevoli sforzi per innalzare gli standard di *cybersecurity* nel settore automobilistico (v. *supra*, par. 4). Sono ora le autorità nazionali che devono vigilare sul rispetto dei menzionati obblighi e divieti, mentre ai legislatori nazionali spetta il compito di prevedere, ove necessario, sanzioni efficaci, proporzionate e persuasive (di natura amministrativa o penale) per far sì che tutti coloro che operino nel settore dell'*automotive* si conformino a tali prescrizioni.
Le misure di sicurezza hanno un ruolo fondamentale nell'assicurare un elevato livello di sicurezza nei veicoli intelligenti, proteggendoli in specie da accessi ed attacchi non autorizzati. Esse, però, andrebbero affiancate da ulteriori misure volte a far sì che, una volta che un soggetto malintenzionato riesca ad introdursi abusivamente nelle reti di comunicazione delle *smart cars* possa prendere il controllo delle parti critiche (sistemi di guida, di frenata, ecc.). A tal fine, tanto a livello sovranazionale quanto nazionale, si dovrebbe prevedere l'obbligo per coloro che operino nel settore dell'*automotive* di adottare un modello di sicurezza in profondità (*security in depth*), da attuarsi cioè su vari strati o livelli, e che, rispetto ai veicoli dotati di sistemi di IA ad alto rischio, sia conforme a quanto stabilito dal recente regolamento europeo 2024/1689 (c.d. *AI Act*)[98].
In questo modo, anche laddove un criminale riuscisse ad accedere ad un veicolo, difficilmente potrebbe riuscire a prenderne il controllo.

[97] *Ibid.* Sulla necessità che alla base di un disastro innominato vi sia una condotta violenta, quale estrinsecazione di una energia fisica, v. i condivisibili rilievi di CORBETTA, *Delitti contro l'incolumità pubblica*, I, *I delitti di comune pericolo mediante violenza*, in *Trattato di diritto penale. Parte speciale*, diretto da Marinucci-Dolcini, Milano, 2003, 629.
[98] V. Considerando 77 Regolamento UE/2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale), pubblicato in GUUE del 12.07.2024.

Ma anche il diritto (penale) gioca un ruolo molto importante, potendo (e dovendo) regolare le attività ed i processi necessari per raggiungere un sistema di (*cyber*)sicurezza in profondità. Solo attraverso un approccio integrato alla *cybersecurity* ed una strategia di prevenzione e contrasto sarà possibile ridurre i rischi cibernetici e limitarne, di conseguenza, gli (eventuali) effetti negativi[99].
In linea con le richiamate indicazioni di fonte sovranazionale, si dovranno privilegiare scelte regolative ed organizzative ispirate ad un approccio proattivo, che favoriscano la prevenzione dei rischi *cyber* e che incrementino la resilienza delle *smart cars* rispetto alle minacce cibernetiche. Si dovrà pertanto richiedere, anche attraverso la previsione di obblighi giuridici, l'adozione di standard ispirati alla *security by design* e di sistemi di gestione della cibersicurezza in tutto il ciclo di vita dei veicoli. Elevando il livello di sicurezza e resilienza dei veicoli, si contribuirà a ridurre costi per riparare i danni causati dai *cyber*-attacchi e per ripristinare le auto compromesse[100].
La rilevanza dei beni giuridici minacciati dagli attacchi alla *automotive cybersecurity* impone inoltre il ricorso al diritto penale per contrastare i comportamenti connotati da un oggettivo disvalore sociale e che costituiscano un concreto pericolo per la sicurezza dei trasporti, per la vita e l'incolumità delle persone coinvolte nella circolazione stradale.
Alla luce delle attuali minacce cibernetiche per le *smart cars* è possibile affermare che la normativa penale vigente nel nostro ordinamento sia sostanzialmente adeguata a tutelare l'*automotive cybersecurity*[101]. Ad una

[99] Rispetto all'importanza di un tale approccio cfr. KANEKO-YAMASHITA-TAKADA-IMAI, *Triad Concurrent Approach Among Functional Safety, Cybersecurity and SOTIF*, in *Journal of Space Safety Engineering*, 2023, 1, 505 ss.
[100] Cfr. OBERTI-ABRATE-SAVINO-PARISI-DI CARLO, *Navigating the Road to Automotive Cybersecurity Compliance*, 2024, 1 ss., 4, consultabile al sito *www.arxiv.org/pdf/2407.00483v1*; ACEA, *Principles of Automotive Cybersecurity*, 2017, consultabile al sito *www.acea.auto/files/ACEA_Principles_of_Automobile_Cybersecurity.pdf*. Sul punto v. anche gli standard tecnici previsti per il settore automobilistico da parte di organismi internazionali (*supra*, par. 4.3).
[101] Cfr. CAPPELLINI, *Profili penalistici*, cit., 343; analogamente, in relazione all'ordinamento tedesco, HILGENDORF, *Automated Driving and the Law*, in *Robotics, Autonomics and the Law*, a cura di Id.-Seidel, Baden-Baden, 2017, 171 ss., 175; rispetto alla legislazione statunitense ALLISON, *You Can't Hack This: The Regulatory Future of Cybersecurity in Automobiles*, in *J. Tech. L. & Pol'y*, 2016, 15 ss., 29 ss.

diversa conclusione si deve giungere, invece, per quanto concerne la protezione del bene collettivo della sicurezza dei trasporti.

Già si è detto (v. *supra*, par. 6.1) come il ricorso alla controversa fattispecie di disastro innominato di cui all'art. 434 c.p., il cui accertamento in sede giudiziale sarebbe, rispetto alle ipotesi di c.d. "dirottamento" di veicoli intelligenti, tutt'altro che agevole.

Onde colmare le lacune legislative oggi esistenti rispetto alla messa in pericolo del trasporto privato minacciato dai *cyber*-attacchi, si dovrebbe intervenire sulla vigente formulazione dell'art. 432 c.p. per adeguarla all'evoluzione del settore. In particolare, si dovrebbe provvedere, in prospettiva *de lege ferenda*, ad eliminare, in punto di tipicità, il requisito della pubblicità dei trasporti, così da estendere l'ambito di applicazione della norma incriminatrice anche al trasporto privato[102]. In questo modo si supererebbe la ingiustificata disparità di trattamento tra trasporto pubblico e privato, che, alla luce del progresso del settore dell'*automotive*, non ha più alcuna ragion d'essere. Nell'alveo dell'art. 432 c.p. potrebbero essere così sussunti anche i cyber-attacchi alle *smart cars* ed ai CAV, che, in un prossimo futuro, in ragione della loro progressiva immissione sulla circolazione stradale, potrebbero mettere in pericolo la sicurezza dei trasporti e, quindi, un numero indeterminato di persone[103].

In prospettiva *de jure condendo*, l'introduzione di nuove (ed ulteriori) fattispecie penali nel settore sempre più complesso e tecnologico dell'*automotive*, dovrà, comunque, poggiare su oggettive evidenze empiriche e criminologiche. Solo in questo modo si potrà evitare il rischio di punire fatti la cui incriminazione, lungi dal rispecchiare concrete forme di aggressione a beni giuridici meritevoli e bisognosi di tutela penale, trovi la sua (prevalente o unica) "giustificazione" in mere suggestioni fantascientifiche o in previsioni catastrofistiche.

---

[102] Si tratta, ad ogni modo, di una norma incriminatrice che si connota per l'indeterminatezza del fatto tipico, essendo indifferenti i modi e gli strumenti mediante i quali si deve mettere concretamente in pericolo la sicurezza dei trasporti, non richiedendo al contempo un effettivo danneggiamento materiale ai veicoli. Cfr. GARGANI, *Il danno qualificato*, cit., 307 ss.

[103] A questa conclusione era già giunta MORGANTE, *In tema di attentato*, cit., 570 ss., la quale muoveva dalla necessità di colmare il (tuttora esistente) vuoto normativo, che impedisce di punire in modo adeguato il lancio di corpi contundenti contro veicoli privati in movimento.