https://doi.org/10.60923/issn.1825-1927/24258 ISSN 1825-1927

Vehicle to Vehicle communications (V2V)

Criticità giuridiche e rischi cibernetici

Casimiro Coniglione [1]

[1] Dipartimento di Giurisprudenza - Università di Modena e Reggio Emilia

Abstract: Il contributo, adottando un approccio informatico-giuridico, analizza i rischi cibernetici dei *Vehicle-to-Vehicle Communications* (V2V): una tecnologia che permette lo scambio di informazioni tra i veicoli, aumentando in questo modo la sicurezza della circolazione stradale e riducendo i rischi di collisione. Introdotti i concetti di "età dei dati", datificazione e i principali standard di comunicazione dei V2V, verranno messe a fuoco alcune criticità di queste tecnologie che riguardano sia la privacy sia la vulnerabilità a specifici *cyber attacks*. Questi ultimi potrebbero ledere l'autonomia decisionale, innescando nei guidatori un *müssen* indotto. Nelle riflessioni conclusive, saranno presi in esame alcuni spunti di riflessione volti a conciliare l'innovazione tecnologica e la tutela degli utenti-conducenti.

Keywords: V2V, privacy, cyber attacks, müssen indotto, cybersecurity

1 Introduzione: "l'età dei dati", la datificazione e i principali standard di comunicazione dei V2V [1]

La rivoluzione tecnologica – che ha avuto e continua ad avere un significativo impatto in tutti i campi della conoscenza[2] – si contraddistingue tanto per la complessità quanto per l'interdipendenza delle nuove tecnologie, promuovendo l'intermediazione digitale e l'interconnessione fra utenti e dispositivi[3].

L'attuale fase storica, come osserva Thomas Casadei, può essere classificata come "l'età dei dati", dal momento che i dati si collocano al centro delle attività dei consociati[4]. Quanto osservato dallo studioso è coerente

casimiro.coniglione@unimore.it (Casimiro Coniglione);

1. Il contributo rientra nelle attività di ricerca del Progetto "Cyber Risks of Vehicle-to-Vehicle Communications" – "CV2V". Bando a cascata sul Programma "Security and RIghts in the CyberSpace" (SERICS). PE000014 finalizzato dall'Unione Europea – "Next Generation UE" su fondi PNRR MUR – M4C2 – Investimento 1.3. Per il costante dialogo e i quotidiani spunti di riflessione si ringraziano i Professori Gianfrancesco Zanetti, Thomas Casadei, Gianluigi Fioriglio e Mirco Marchetti, *Principal Investigator* (P.I.) del Progetto "CV2V". Un doveroso ringraziamento è rivolto ai *referees* per le puntuali osservazioni e i generosi suggerimenti forniti al sottoscritto, consentendo così di chiudere alcuni passaggi fondamentali nel contributo.

2. M. Mancarella (a cura di), *Lineamenti di informatica giuridica*, Tangram, Trento, 2024, p. 83.

3. M. Martoni, *Un'autonomia ostacolata. Limiti cognitivi, incompetenze e design ingannevoli nella trasformazione digitale*, in *Sociologia del diritto*, Vol. 51, 1, 2024, pp. 7-32, in part. pp. 9-10.

4. Th. Casadei, *Rights in the age of data*, in F. Pedrini (ed.), *Law in the age of Digitalization*, Aranzadi, Madrid, 2024, pp. 45-64, in part. pp. 46-47. Inoltre, cfr. G. Contissa – F. Godano – G. Sartor, *Computation, Cybernetics and the Law at the Origins of Legal Informatics*, in S. Chiodo – V. Schiaffonati (eds.), *Italian Philosophy of Technology. Socio-Cultural, Legal Scientific and Aesthetic. Perspectives on Technology*, Springer, Cham, 2021, pp. 91-110; M. Hildebrandt – B. van den Berg (eds.), *Information, Freedom and Property. The philosophy of law meets the philosophy of technology*, Routledge, Abingdon, 2016; U. Pagallo – M. Durante, *The Philosophy of Law in an Information Society*, in L. Floridi (ed.), *The Routledge Handbook of Philosophy of Information*, Routledge, Abingdon, 2016, pp. 396-407.

con la decisiva circostanza che la normatività[5] – un tempo identificata unicamente nell'autorità statale e nel diritto codificato[6] – assume anche forme digitali: i dati, gli algoritmi e l'architettura complessiva dei sistemi informatici influenzano sia i comportamenti sia le relazioni del *démos*[7].

Proseguendo su questo orizzonte argomentativo, il processo tecnologico della datificazione (*datafication*) trasforma le azioni e le interazioni dei consociati in dati digitali quantificabili e ciò è «la precondizione essenziale per l'applicazione di strumenti e tecniche di estrazione della conoscenza al fine di coadiuvare, o determinare *tout court*, i processi decisionali destinati a produrre modificazioni della realtà (naturale o digitale) che sono, a loro volta, datificate o dataficabili»[8]. Di conseguenza, è possibile portare avanti l'idea che la datificazione incida sia sul *modus vivendi*[9] (stile di vita) sia sull'*ars pensandi*[10] (arte del pensare) dei consociati.

Queste brevi riflessioni trovano un riscontro nella costante interazione tra la dimensione digitale e quella fisica grazie all'*Internet of Things* (IoT – Internet delle Cose), dispositivi connessi alla rete che interagiscono con la realtà fisica mediante sensori e attuatori, perfezionando la raccolta e l'analisi dei dati derivanti da diverse fonti[11].

In questo specifico senso, i sistemi *Vehicle-to-Vehicle* (V2V) sono una peculiare forma di IoT: si basano sul continuo scambio di dati fra i veicoli per ottimizzare la sicurezza stradale nonché il coordinamento complessivo della mobilità[12]. Essi non solo rappresentano un caso di interazione tra dinamiche digitali e fisiche, ma sono anche una modalità della *smart mobility*, in quanto delineano l'infrastruttura digitale della mobilità[13].

Pare opportuno impostare l'indagine su tre livelli distinti ma collegati fra loro: una ricostruzione tecnico-descrittiva dei principali standard di comunicazione dei V2V; le criticità sulla protezione dei dati personali e i principali *cyber attacks* (attacchi informatici) a cui tali sistemi sono esposti, con cenni sull'imputazione delle responsabilità nei casi di collisioni; una riflessione filosofico-giuridica volta a interpretare le eventuali forme

5. Oppure, per dirlo *à la* Frederick Schauer (1946-2024), la forza normativa. F. Schauer, *La forza del diritto* (2015), Mimesis, Milano-Udine, 2016.

6. Al riguardo: A.C. Amato Mangiameli, *Stati post-moderni e diritto dei popoli*, Giappichelli, Torino, 2004.

7. M.N. Campagnoli – M. Farina, *Identità digitale e intelligenza artificiale: tra regolazione, poteri asimmetrici e sfide per il futuro*, in *Journal of Ethics and Legal Technologies*, Vol. 7, 1, 2025, pp. 81-115, in part. pp. 82-83.

8. C. Sarra, *L'uomo dato. Antropologia (giuridica) della datificazione*, in F. Casa – S. Gaetano – G. Pascali (a cura di), *Dignità umana nell'era dell'intelligenza artificiale*, il Mulino, Bologna, 2025, p. 158. Cfr. Id., *Dignità umana nell'era dell'intelligenza artificiale e della datificazione*, Kront, Roma, 2025.

9. A. Gehlen, *L'uomo nell'era della tecnica. Problemi socio-psicologici della civiltà industriale*, trad. it., SugarCo, Milano, 1967, p. 12.

10. H. Jonas, *Dalla fede antica all'uomo tecnologico* (1974), trad. it., il Mulino, Bologna, 1991, p. 9.

11. Per l'IoT la letteratura scientifica è assai estesa. Ciò nondimeno, per un primissimo approccio, si rinvia e*x multis*: L. Paseri, *Il governo dei dati. Interesse pubblico, altruismo e partecipazione*, Giappichelli, Torino, 2025; E. Susco, *IoT*, in A.C. Amato Mangiameli – G. Saraceni (a cura di), *Cento e una voce di informatica giuridica*, Giappichelli, Torino, 2023, pp. 292-296; L. Denardis, *Internet in ogni cosa. Libertà, sicurezza e privacy nell'era degli oggetti iperconnessi*, Luiss University Press, Roma, 2021; A. Maceratini, *Dall'Internet of Things alle Smart Roads. Riflessioni informatico-giuridiche su strade intelligenti, veicoli automatici e connessi*, in *Rivista elettronica di Diritto, Economia, Management*, 3, 2019, pp. 71-91; F. Faini, *Big data e Internet of Things: data protection e data governance alla luce del regolamento europeo*, in G. Cassano – V. Colarocco – G.B. Gallus – F.P. Micozzi (a cura di), *Il processo di adeguamento al GDPR europeo. Aggiornato al D. lgs 10 agosto 2018*, Giuffrè, Milano, 2018, pp. 259-280; A. Rayes – S. Salam, *Internet of Things. From Hype to Reality*, Springer, Cham, 2017; U. Pagallo – M. Durante – S. Monteleone, *What is new with the Internet of Things in Privacy and data protection? Four legal challenges on sharing and control in IoT*, in R. Leenes – R. van Brakel – S. Gutwirth – P. de Hert (eds.), *(In)visibilities and Infrastructures*, Springer, Cham, 2017, pp. 59-79.

12. Insieme ai sistemi V2I (*Vehicle-to-Infrastructure*), ossia veicoli che interagiscono e scambiano dati con le infrastrutture, i V2V rientrano nel genere più ampio di *Internet of Vehicles* (Internet dei Veicoli). Per un ampio approfondimento sul tema: N. Magaia – G. Mastrorakis – G. Mavromoustakis – E. Pallis – E.K. Markakis (eds.), *Intelligent Technology for Internet of Vehicles*, Springer, Cham, 2021.

13. Sulla *smart mobility* cfr. A. Palladino, *Sharing, Data and Smart Mobility. Towards Innovative Urban Paradigms*, Key Editore, Milano, 2024, pp. 33-39; N. Miniscalco, *L'Intelligenza Artificiale in movimento. L'impatto sui diritti costituzionali della smart mobility*, Wolters Kluwer, Milano, 2024.

di condizionamento dell'urgenza decisionale generate dagli effetti degli attacchi informatici. Nel far ciò sarà proposto il concetto di *müssen* indotto, interpretabile quale categoria analitico-descrittiva.

L'esposizione dei principali metodi di interazione dei V2V consente, da una parte, di comprendere le ragioni per cui tali sistemi possiedono un'intrinseca vulnerabilità e, dall'altra parte, gli effetti che possono produrre nei confronti degli utenti-conducenti.

Gli standard di comunicazione dei sistemi V2V sono molteplici, variano a seconda delle specifiche architetture tecnologiche adottate. In questa sede si esporranno i più noti e discussi dalla letteratura scientifica[14].

Il DSRC (*Dedicated Short Range Communication*) – assieme al GPS (*Global Positioning System*) in qualità di tecnologia di supporto – offre trasmissioni precise delle posizioni dei veicoli attraverso scambi comunicativi[15], ha una bassa latenza, portata limitata ed elevata affidabilità nelle comunicazioni a corto raggio[16]. Gli infrarossi (*infrared*) assicurano affidabilità e facilità delle trasmissioni. Il *Bluetooth* ha un ridotto consumo energetico, nonché una buona sicurezza nelle trasmissioni delle comunicazioni. L'UWB (*Ultra-Wideband*) possiede ottime potenzialità nel contrastare le interferenze. Il *mm Wave* (*millimeter Wave*) assicura la trasmissione di dati con una velocità altissima. La C-V2X (*Cellular Vehicle-to-Everything*) – con l'ausilio delle reti 4G e 5G – migliora l'efficienza comunicativa nello scambio di informazioni fra veicoli e infrastrutture.

Un'ulteriore osservazione va effettuata sulla C-V2X, la cui tipicità risiede nell'incentrarsi su una comunicazione bidirezionale, consentendo la condivisione delle informazioni critiche. In virtù del fatto che la trasmissione dei dati ha luogo in un breve raggio, i rischi di collisione vengono notevolmente attenuati e ciò grazie agli avvisi in tempo reale come le segnalazioni sulla mancata distanza di sicurezza fra i veicoli, l'eccessiva vicinanza al margine della carreggiata o la presenza di veicoli nelle prossimità con la precisa indicazione dei loro movimenti[17].

I meriti di questo standard – al di là degli aspetti squisitamente tecnici – risiedono anche a livello giuridico: garantisce la privacy, l'autenticazione dei messaggi di sicurezza, flessibilità dei *network* e dei programmi sicuri che adoperano metodologie simili (per esempio, i V2V o i V2I), l'osservanza della *cybersecurity* (sicurezza informatica), nonché il vantaggio di connessioni quasi istantanee[18].

Ciò nondimeno, l'altra faccia della medaglia dei sistemi V2V evidenzia come l'interconnessione tra veicoli, utenti e infrastrutture comporti criticità sotto il profilo della protezione dei dati e un ampliamento della superficie di esposizione agli attacchi informatici.

2 Criticità sulla privacy e i principali *cyber attacks* ai V2V. Brevi cenni sull'imputazione delle responsabilità

Come discusso, la bidirezionalità e la trasmissione continua dei dati sono le qualità distintive dei V2V. Tuttavia, persistono alcuni assi di tensione, in modo particolare per la protezione dei dati dei conducenti e la vulnerabilità a specifici attacchi informatici.

14. In questo senso: M. El Zorkany – A. Yasser – A.I. Galal, *Vehicle to Vehicle "V2V" Communication: Scope, Importance, Challenges, Research Directions and Future*, in *The Open Transportation Journal*, 14, 2020, pp. 86-98.

15. K.B. Yogha, *A Study of V2V Communication on VANET: Characteristic, Challenges and Research Trends*, in *JISA (Jurnal Informatika dan Sains)*, Vol. 4, 1, 2020, pp. 46-58.

16. Per la puntuale analisi di questo standard e del suo protocollo di comunicazione, l'IEEE 802.11p., si veda S. Shrivastava, *V2V Vehicle Safety Communication*, in R. Miucic (ed.), *Connected Vehicles. Intelligent Transportation Systems*, Springer, Cham, 2019, pp. 117-155.

17. J. Chen, *Comparison and Optimization of DSRC and C-V2X Technologies: Current Status, Challenges and Future Prospects*, in *Academic Journal of Science and Technology*, Vol. 13, 2, 2024, pp. 42-50.

18. F. Lyu – M. Li – X. Shen, *Networking for Road Safety*, Springer, Cham, 2020, pp. 1-9.

Iniziando dal tema della *privacy*, è evidente che nella raccolta, nell'elaborazione e nel trattamento dei dati permane una condizione di "incertezza del diritto"[19]. Difatti, la trasmissione di messaggi BSM[20] (*Basic Safety Messages*) nei V2V contiene informazioni importanti (si pensi alla direzione e alla velocità) che consentono una re-identificazione dei conducenti, con l'obiettivo di tracciare gli spostamenti e costruire profili comportamentali dei guidatori.

Sebbene i dati vengano regolarmente pseudonimizzati per limitarne la tracciabilità, è sempre possibile un collegamento con gli identificatori temporanei per abbinarli con altre fonti di dati (telecamere urbane o i sensori stradali). In questo modo, vengono lesi i principi sanciti dall'art. 5 – ossia la liceità, la correttezza, la trasparenza e la limitazione della finalità del trattamento dei dati – sia dell'art. 25 del GDPR: la *privacy by design* e *by default*.

Com'è noto, la *privacy by design* prevede la protezione dei dati sin dalla fase di progettazione dei sistemi, limitazioni nelle finalità del trattamento e la predisposizione delle misure tecniche più adeguate[21]; invece, la *ratio* che sta alla base della *privacy by default* è di garantire che – per impostazioni predefinite – vengano raccolti e trattati unicamente i dati necessari per fini specifici del sistema[22].

Peraltro, i dati V2V possono essere adoperati per il *secondary use* (l'uso secondario dei dati) e la profilazione predittiva[23]. Quest'ultima può distinguersi in comportamentale se descrive gli stili di guida dei conducenti, geografica quando vengono vagliati gli spostamenti e socio-economica per lo studio delle condizioni dei guidatori.

Ragionando in questi termini, è lecito ipotizzare che le finalità originarie del trattamento dei dati siano ampiamente oltrepassate, creando i presupposti di una dataveglianza[24] (*dataveillance*) dove la logica predittiva gioca un ruolo centrale: classificazioni e rivelazioni delle preferenze degli utenti rappresentano gli elementi costitutivi del procedimento[25].

Dunque, la prima tensione riguarda la tutela della riservatezza dei dati degli utenti nei sistemi V2V[26].

19. Per l'ampia trattazione di questa importante tematica: G. Gometz, *L'incertezza del diritto*, Giappichelli, Torino, 2024.

20. Fondamentali, sui messaggi BSM, le riflessioni di F. Pollicino – D. Stabili – M. Marchetti, *On the effectiveness of BSM communications in V2V emergency scenarios*, in *IEEE 95th Vehicular Technology Conference*, Helsinki, 2022, pp. 1-5.

21. Imprescindibile il riferimento a: A. Cavoukian, *Privacy by design*, IPC Publications, Ottawa, 2009. Cfr., inoltre, U. Pagallo, *Privacy e design*, in *Informatica e diritto*, Vol. XVIII, 1, 2009, pp. 123-134; Id., *On the Principle of Privacy by Design and its Limits: Technologies, Ethics and Rule of Law*, in S. Gutwirth – R. Leenes – P. de Hert – Y. Poullet (eds.), *European Data Protection: In Good Health?*, Springer, Cham, 2012, pp. 331-346.

22. Riguardo la *privacy by default*: F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla direttiva 95/46 al nuovo Regolamento europeo*, Giappichelli, Torino, 2016; M. Farina, *Il cloud computing in ambito sanitario tra security e privacy*, Giuffrè, Milano, 2019, pp. 1-10.

23. La profilazione, ad avviso di Giovanni Ziccardi, fa sì che «l'essere umano oggi è in *competizione* con le macchine che trattano i suoi dati. Macchine che riescono a recuperare informazioni e a elaborare dati che sono in grado di distinguere, attorno all'individuo, un profilo (o "corpo elettronico" come scriverebbe Stefano Rodotà) ancora più preciso di come l'essere umano conosca sé stesso, e capace di prevedere, perché no, di orientare i comportamenti» (G. Ziccardi, *Diritti digitali. Informatica giuridica per le nuove professioni*, Raffaello Cortina Editore, Milano, 2022, p. 69).

24. Roger Clarke, autore del lemma in esame, ritiene che la dataveglianza sia «la sistematica investigazione o monitoraggio delle azioni o delle comunicazioni di una o più persone cui scopo primario è, generalmente, collezionare informazioni su loro, loro attività» (R. Clarke, *Information technology and dataveillance*, in *Communication of the ACM*, Vol. 31, 5, 1988, p. 499). Oltre a ciò, cfr. D. Lyon, *L'occhio elettronico. Privacy e filosofia della sorveglianza*, trad. it., Feltrinelli, Milano, 1997; H.F. Nissenbaum, *Privacy in context: technology, policy and the integrity of social life*, Stanford University Press, Redwood City, 2009; C. Blengino – S. Mondino, *Smart cities and smart citizens: trasformazioni e rappresentazioni della sicurezza nell'era della dataveglianza*, in R. Brighi – S. Zullo (a cura di), *Filosofia del diritto e nuove tecnologie. Prospettive di ricerca tra teoria e prassi*, Aracne, Roma, 2015, pp. 41-56; P. Tincani, *Sorveglianza e potere. Disavventure dell'asimmetria cognitiva*, in *Ragion pratica*, 1, 2018, pp. 51-78; P. Perri, *Sorveglianza elettronica, diritti fondamentali ed evoluzione tecnologica*, Giuffrè, Milano, 2020, pp. 22-28.

25. L. Corso, *Breve tassonomia dei rapporti fra Intelligenza Artificiale e diritto. Tre questioni*, in *AI Law. International review of Artificial Intelligence*, 2, 2025, pp. 204-222.

26. F. Costantini – N. Thomopoulos – F. Steibel – A. Curi – G. Lugano – T. Kovacikova, *Autonomous vehicles in a GDPR era: An international comparison*, in *Advanced in Transport Policy and Planning*, Vol. 5, 2020, pp. 192-213, in part. p. 197.

Una seconda criticità è connessa a un'intrinseca vulnerabilità[27] dei sistemi a specifici *cyber attacks*, i quali non rilasciano i loro effetti unicamente nella sfera virtuale-cibernetica degli utenti, bensì anche in quella fisica, relazionale e sociale[28]. Questa sovrapposizione nelle sfere costituisce il risultato dell'interconnessione fra utenti e dispositivi, all'interno della quale la vulnerabilità – che è un rischio diffuso per l'intero *démos*[29] – è aumentata a causa di un «allargamento della superficie di esposizione prodotto dalla fusione tra strati informatici e dispositivi in riferimento a spazialità, temporalità, inferenzialità, istituzionalità, asimmetricità»[30].

Tra gli attacchi a cui i sistemi V2V sono più esposti vi è, in primo luogo, lo *spoofing*. In questo attacco l'aggressore trasmette messaggi falsi per ingannare i veicoli e spingerli a compiere manovre pericolose[31]; nel *Denial of Service* – sovraccaricando la rete V2V – viene troncata la comunicazione fra i veicoli[32]; l'attacco *Man-in-the-Middle* (MitM) intercetta e modifica le comunicazioni, allo scopo di compromettere i dati[33]; nel CAN *Injection Attack* – che riguarda il dominio intraveicolare – vengono manipolati i segnali dei veicoli, influenzando i sistemi dello sterzo e dei freni[34]; infine, anche se non è classificabile un attacco diretto ai V2V, va segnalato l'*Unauthorized Remote Access*, poiché sfrutta le vulnerabilità dei sistemi di *infotainment* e consente l'accesso non autorizzato ai sottosistemi interni, interferendo indirettamente con le comunicazioni V2V[35].

Siffatte vulnerabilità, derivanti dagli attacchi menzionati sopra, sollevano perplessità sulle responsabilità nei casi di collisioni. Ci si dovrebbe domandare se queste possono essere imputate al produttore, all'operatore o al guidatore? I quesiti posti hanno un loro fondamento, è possibile intravedere un potenziale rischio distribuito lungo la catena socio-tecnica: il singolo attacco potrebbe compromettere l'intera rete dei veicoli.

Pur non essendo questa la sede per discutere nel dettaglio delle responsabilità – le quali meriterebbero un'articolazione più ampia – si può ritenere che il produttore incorra in responsabilità laddove non abbia adempiuto gli obblighi in materia di *cybersecurity*, immettendo nel mercato prodotti difettosi in violazione degli standard R155[36] e dell'ISO/SAE 21434[37]. In questo orizzonte normativo, va menzionata la Direttiva sulla responsabilità per danno da prodotti difettosi (2024/2853), la quale estende il regime di responsabilità

27. Quando si argomenta della vulnerabilità, è utile distinguerla in due tipologie: in una prospettiva filosofico-giuridica è la predisposizione ad essere danneggiati da eventi, minacce, attacchi fisici o psicologici; nella prospettiva informatico-giuridica è da intendersi come una propensione – in virtù dell'architettura complessiva di determinati sistemi informatici – agli attacchi informatici. Per la filosofia del diritto, *ex multis*, M.G. Bernardini – B. Casalini – O. Giolo – L. Re (a cura di), *Vulnerabilità: etica, politica, diritto*, Carocci, Roma, 2018; A. Furia – S. Zullo (a cura di), *La vulnerabilità come metodo. Percorsi di ricerca tra pensiero politico, diritto ed etica*, Carocci, Roma, 2020; A. Di Giandomenico – C. Diodati – F. Ricci, *Vulnerabilità come risorsa e valorizzazione. Profili giuridici, sociologici ed etico-politici*, Mimesis, Milano-Udine, 2021; T. Serra, *Vulnerabilità e etica della cura*, in A. Di Giandomenico (a cura di), *Etsi Deus non daretur … Scritti in memoria di Serenella Armellini*, Giappichelli, Torino, 2023, pp. 459-466; Gf. Zanetti, *Equality and Vulnerability in the Context of Italian Political Philosophy. Italian Efficacy*, Springer, Cham, 2023. Per l'informatica giuridica: R. Brighi, *Cybersecurity. Scenari tecnologici e regolamentazione di un'area in espansione*, in Th. Casadei – S. Pietropaoli (a cura di), *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, Wolters Kluwer, Milano, 2024, pp. 75-86, in part. pp. 77-79.

28. R. Brighi – V. Ferrari, *(Cyber)sicurezza e infanzia digitale. Oltre la protezione, verso un uso critico e consapevole della tecnologia*, in Th. Casadei – V. Barone – B. Rossi (a cura di), *Giovani in rete. Guida per un uso consapevole delle tecnologie*, Giappichelli, Torino, 2025, pp. 15-30, in part. pp. 25-29.

29. P. Pettit, *Il repubblicanesimo* (1977), trad. it., Feltrinelli, Milano, 2000, p. 152.

30. G. Fioriglio, *Vulnerabilità aumentata. Diritto, cura e algoritmi nell'era della salute digitale*, Mucchi Editore, Modena, 2025, p. 40.

31. ENISA, *ENISA Threat Landscape 2024*, Heraklion, 2024, p. 115.

32. Ivi, pp. 78-79.

33. ENISA, *Identifying Emerging Cyber Security Threats and Challenges for 2030*, Heraklion, 2023, p. 14 e p. 21.

34. C. Smith, *The Car Hacker's Handbook. A Guide for the Penetration Tester*, No Starch Press, San Francisco, 2016, pp. 148-156.

35. S. Kim – R. Shrestha, *Automotive Cyber Security. Introduction, Challenges and Standardization*, Springer, Cham, 2020, pp. 67-96.

36. L'UNECE *Regulation* n. 155 (R155) impone rigorosi requisiti di sicurezza informatica per i veicoli, imponendo ai produttori la messa in atto di una *Cybersecurity Management Systems* (CMS – Sistema di Gestione della Cibersicurezza) per l'intero ciclo di vita del veicolo.

37. Integra il R155 e offre un quadro operativo per la *cybersecurity*, dettando precise linee guida per i *cyber risks* in tutte le fasi: dalla progettazione fino allo smaltimento dei sistemi elettronici nei veicoli.

oggettiva ai sistemi *software*. Inoltre, è imprescindibile il riferimento alla Direttiva NIS2 (2022/2555), che disciplina gli obblighi di sicurezza informatica nel settore dei trasporti e impone agli operatori l'adozione delle misure tecniche e organizzative più adeguate alla gestione dei rischi nonché la notifica degli incidenti rilevanti alle autorità competenti.

L'operatore della rete, dal canto suo, è responsabile se l'attacco cibernetico è la conseguenza delle vulnerabilità della rete V2V, senza che siano state fornite le necessarie misure di sicurezza. I guidatori non possono essere considerati responsabili[38] se le loro condotte sono la conseguenza dei *cyber attacks*, salvo che abbiano agito con grave negligenza in casi[39] di mancato aggiornamento del *software* o uso improprio dei sistemi V2V.

L'accenno all'imputazione delle responsabilità chiarisce come il rapporto che si instaura fra guidatori e sistemi V2V è fondato su strutture codificate indifferenti rispetto al senso etico delle relazioni[40], il cui significato è ricavabile esclusivamente in modalità oggettivo-verificabili[41].

È importante ragionare sulle conseguenze dell'eventuale influenza esercitata da questi sistemi nei casi in cui i *cyber attacks* compromettano le comunicazioni dei V2V, per la ragione che le scelte degli utenti «sono trasmutate in nient'altro che nei contenuti impressi nel dataismo e dalle interazioni dei quanti alle sue condotte, divenute esecutive-innocenti e pertanto più creative responsabili»[42].

3 *Müssen* indotto?

In tempi recenti la letteratura informatico-giuridica e giusfilosofica si sta interrogando in forme sempre più radicali[43] sulla capacità delle tecnologie digitali di produrre un mutamento di paradigma, al punto tale da incidere nel rapporto tra diritto, decisione e autonomia[44].

Alla luce delle crescenti interazioni tra sistemi *Vehicle-to-Vehicle* (V2V) e conducenti, nonché dell'ampliamento della superficie di vulnerabilità derivante dalla stratificazione degli ambienti informatici, i *cyber attacks* possono produrre effetti che non rimangono confinati nella dimensione digitale, ma possono invadere la sfera d'azione degli individui.

Non è una casualità che si discuta di "normatività tecnologica" che – per quanto non possa identificarsi in senso stretto con la normatività giuridica – esercita una forza capace di orientare le modalità decisionali degli utenti. D'altronde, le tecnologie condividono con il diritto una funzione regolativa, svolgono il ruolo di tecniche comportamentali e condizionano le scelte degli agenti tramite strutture codificate e procedure predefinite[45].

38. Del resto, è coerente con quanto ipotizzato da Alf Ross (1899-1979), in quanto l'imputazione della responsabilità per un'azione può essere attribuita al soggetto al compimento di certe condizioni: capacità, occasione e motivazione nella commissione del fatto. A. Ross, *Colpa, responsabilità e pena* (1970), trad. it., Giuffrè, Milano, 1982, p. 264. Le medesime argomentazioni vengono riprese dal filosofo del diritto analitico U. Scarpelli, *La responsabilità politica*, in R. Orecchia (a cura di), *La responsabilità politica, diritto, tempo. Atti del XIII Congresso Nazionale (Pavia-Salice Terme 28-31 maggio 1981)*, Giuffrè, Milano, 1982, pp. 43-95.

39. I sistemi V2V sono fondamentali nei veicoli a guida autonoma, in modo particolare a partire dal livello 3 (automazione condizionata). Ciò solleva interrogativi su eventuali nuovi profili della responsabilità nei casi di collisioni. Per siffatte argomentazioni si rinvia a G. Contissa – F. Lagioia – G. Sartor, *Liability and automation: legal issues in autonomous cars*, in *Network Industries Quarterly*, Vol. 20, 2, 2018, pp. 21-26. Sul nesso responsabilità e assetto socio-tecnico, G. Contissa – G. Sartor, *Liability and automation in socio-technical systems*, in B. Wagner – M.C. Ketteman – K. Vieth-Diltmann – S. Montgomery (eds.), *Handbook on Human Rights and Digital Technology. Global Politics, Law and International Relations*, Elgar, Cheltenham-Northampton, 2025, pp. 222-242.

40. M. Catanzariti, *Etica "artificiale": un modello regolatorio*, in *Ars Interpretandi*, 1, 2021, pp. 165-179.

41. F. Romeo, *Il dato digitale e la natura delle cose*, in A. Ballarini (a cura di), *Diritti interessi ermeneutica*, Giappichelli, Torino, 2012, pp. 102-103.

42. B. Romano, *Opera Omnia. Ragione sufficiente e diritto. Dataismo e teoria dei quanti*, Giappichelli, Torino, 2023, pp. 4-5.

43. Cfr. K. Jaspers, *La fede filosofica di fronte alla rivelazione*, trad. it., Longanesi, Milano, 1970.

44. Si veda al riguardo: R. Brownsword, *Law 3.0. Rules and Technology*, Routledge, Abingdon, 2021; T. Gazzolo, *Che cos'è la forza della legge?*, in *Diritto pubblico*, 3, 2023, pp. 861-891.

45. M.R. Ferrarese, *Scrittura digitale e normatività tecnologica*, in *Quaderni costituzionali*, 1, 2026, pp. 65-82, in part. pp. 67-69.

È in questo quadro teorico che si propone il concetto di *müssen* indotto, da intendersi come categoria analitico-descrittiva priva di qualsivoglia valenza normativa o prescrittiva, riconducibile a uno strumento euristico per descrivere dinamiche che emergono nei sistemi V2V.

Si precisa che la categoria si distingue dalla coercizione giuridica o fisica, non implica in alcun modo un vincolo opponibile all'agente. Si differenzia anche dal *nudging*, perché non parte dall'assunto di una progettazione intenzionale di scelte; a sua volta, non può nemmeno ridursi alla disinformazione: la sua portata non si esaurisce nel solo piano cognitivo, bensì abbraccia l'intera struttura tecnico-informazionale della percezione dell'urgenza decisionale. In sostanza, è una struttura percettiva dell'urgenza decisionale filtrata dall'architettura tecnica.

La scelta del verbo "indurre", che deriva dal latino *inducĕre* e significa "introdurre", "condurre dentro" o "suscitare", vuole indicare un processo di eterodirezione informazionale del comportamento.

L' "indotto" ha differenze assai nette rispetto al *müssen* kelseniano[46]. Com'è noto, per Hans Kelsen (1881-1973) il *müssen* esprime una necessità logico-formale interna al sistema giuridico, distinta dalla causalità naturale ma caratterizzata da una connessione necessaria propria della struttura normativa[47]. L'esempio classico proposto dal giurista austriaco per la comprensione del concetto è quello dei metalli: se sottoposti al calore essi si dilatano; analogamente, nel modello kelseniano la relazione tra presupposto e conseguenza è ricostruita come necessità sistemica interna all'ordinamento.

Nel *müssen* indotto, invece, la "necessità" non deriva né dalla struttura del diritto né da una regolarità naturale, ma dal condizionamento esterno che orienta il comportamento dell'agente senza tradursi materialmente in vincolo giuridico.

Per la classificazione concettuale della categoria si possono mettere a fuoco tre criteri: la presenza di un'informazione proveniente dai sistemi tecnici interconnessi (i V2V); la percezione di un'urgenza operativa non controllabile nel breve periodo dall'agente; l'attivazione di una condotta correttivo-preventiva dell'agente priva di una mediazione deliberativa pienamente autonoma. Siffatte "condizioni" si distinguono, per un verso, dalle ordinarie forme di influenza informativa e, per un altro verso, dalle ipotesi della coercizione giuridica.

A titolo esemplificativo del *müssen* indotto, si pensi all'attacco *spoofing* nei sistemi V2V: il veicolo A trasmette al veicolo B un messaggio sulla necessità di diminuire la velocità. L'agente malevolo intercetta e falsifica il messaggio, riproponendolo come se fosse proveniente da A, segnalando l'urgenza della frenata per evitare l'imminente collisione. Il conducente del veicolo B, attribuendo autenticità al segnale ricevuto da A, effettua una brusca decelerazione con significativi effetti fisici.

Nell'esempio descritto sopra, la condotta dell'agente non sembra riconducibile all'obbligo giuridico o a una decisione pienamente informata, piuttosto sembrerebbe l'effetto vincolante di un'informazione tecnicamente mediata che assume la forma di una necessità operativa. In considerazione di ciò, potrebbe risultare uno scarto fra autonomia della decisione ed eterodirezione informazionale. Il suddetto scarto è il nucleo essenziale del *müssen* indotto ipotizzato in questa sede.

Il dover-agire non pare radicarsi su principi morali o su atti della ragione[48], anzi è collegato alla coerenza sintattica del segnale e dalla traduzione della conoscenza in schemi formalizzati tipici delle architetture digitali[49], confondendo l'agente su ciò che deve e ciò che appare.

46. Cfr. H. Kelsen, *Che cos'è la dottrina pura del diritto?*, a cura di T. Gazzolo, La nave di Teseo, Milano, 2022; Id., *Teoria generale delle norme* (1979), a cura di M.G. Losano, Einaudi, Torino, 1985. Per una completa esposizione del *Sein* e *Sollen* in Kelsen: T. Gazzolo, *Essere/dover essere. Saggio su Hans Kelsen*, FrancoAngeli, Milano, 2016.

47. E. Pattaro, *Filosofia del diritto. Diritto. Scienza giuridica* (1978), a cura di M. La Torre, Rubbettino, Soveria Mannelli, 2023, p. 72.

48. K.A. Appiah, *Experiments in Ethics*, Harvard University Press, Cambridge, 2008.

49. Cfr. R. Kowalski, *Legislation as Logic Programs*, Imperial College London, 1991; G. Sartor, *Linguaggio giuridico e linguaggi di programmazione*, Clueb, Bologna, 1992.

Lo scopo della categoria proposta non è descrivere un errore informativo e neppure una strategia di orientamento delle scelte, ma quello di gettare luce su una potenziale forma di necessità percettiva generata dall'architettura tecnico-informazionale.

Il *müssen* indotto – oltre la sua elaborazione teorica e nei casi più estremi – può ricondursi a una categoria descrittiva utile all'analisi dei fenomeni di eterodirezione informazionale dell'agire, nei quali viene prodotta una percezione di un'urgenza decisionale vissuta dal soggetto come vincolante, in ragione dell'assetto tecnico-informazionale della comunicazione V2V.

4 Riflessioni conclusive

Le argomentazioni svolte in questa sede sembrano confermare che i sistemi V2V rientrano nell'età dei dati e nel processo di datificazione, sia per produrre conoscenza e modifiche sia per ottimizzare la sicurezza stradale e la mobilità. Ciò nonostante, non sono esenti da criticità sul versante della privacy e della *cybersecurity*.

Si intendono suggerire alcuni spunti di riflessione informatico-giuridici, perché i benefici di questo approccio sono quelli di riportare unità nelle frammentarie tendenze dei diversi rami del diritto, sottolineando le criticità e le specificità[50].

Il primo spunto di riflessione è dedicato alla legislazione. Preso atto del pregresso disimpegno regolatorio, in ossequio all'orientamento neoliberale[51] del mercato, l'attuale approccio del legislatore nelle tecnologie è *top down*: risulta necessaria l'emanazione di nuove leggi per regolamentare i nuovi fenomeni[52]. La conferma di questo approccio è l'attuale orientamento della legislazione europea, conscia che la regolamentazione delle nuove tecnologie possa ruotare su principi chiari, definiti, sviluppati in modo flessibile, incentivando in questo modo la partecipazione attiva al processo legislativo e aumentando sia la fiducia sia l'assunzione delle responsabilità[53].

Sarebbe auspicabile non solo l'estensione delle normative esistenti come parte integrante dei sistemi di sicurezza dei V2V, ma si potrebbero introdurre normative *ad hoc* per le comunicazioni V2V, assicurando in questo modo precisi standard di sicurezza e protocolli di autenticazione. Del resto, in via legislativa sarebbe opportuno immaginare nuovi schemi di imputazione delle responsabilità nell'utilizzo dei sistemi V2V, in grado di tenere conto delle molteplicità dei soggetti coinvolti[54].

Il secondo spunto di riflessione, dedicato al rigoroso rispetto del GDPR, vorrebbe suggerire una strategia integrata basata su pseudonimi temporanei, crittografia avanzata e controlli di accesso con la PKI (*Public Key Infrastructure*) per l'autorizzazione dei veicoli, *audit* e trattamenti *compliance* nel *design* dei sistemi V2V. In questo frangente, un ruolo decisivo può essere svolto dalla collaborazione fra pubblico e privato.

Un esempio proficuo di collaborazione potrebbe essere il collegamento dei sistemi V2V al DATEX II (*Data Exchange Infrastructure Initiative*): lo standard europeo per lo scambio di dati su traffico e mobilità. Siffatta prospettiva incrementerebbe la *governance* dei dati, attuando un approccio che vada dalla privacy *by books* alla privacy *in actions*[55]. Il dialogo fra tecnici e pratici potrebbe facilitare l'elaborazione di soluzioni efficaci, sostenibili nonché capaci di rispondere alla repentinità dei cambiamenti tecnologici[56].

50. U. Pagallo, *Introduzione*, in Id. (a cura di), *Prolegomeni d'informatica giuridica*, Cedam, Padova, 2003, pp. 1-66, in part. p. 1.

51. Cfr. O. Giolo, *Il diritto neoliberale*, Jovene, Napoli, 2020.

52. R. Calo, *Robotics and the Lessons of Cyberlaw*, in *California Law Review*, 103, 2015, pp. 513-564.

53. A. Punzi, *"Accolse l'uomo come opera di natura indefinita". Note su esperienza giuridica e nuovo ordine delle intelligenze*, in *Rivista di filosofia del diritto*, 1, 2025, pp. 21-32, in part. pp. 29-30.

54. Cfr. M.N. Campagnoli – M. Farina, op. cit., p. 93.

55. Cfr. G. Fioriglio, *Trattamento dei dati sanitari e ricerca medica: profili informatico-giuridici e istituzionali nel contesto europeo*, in *Jura Gentium*, 2, 2025, pp. 1-30, in part. p. 30.

56. A questo proposito, sono state scritte pagine importanti da R. Borruso, *L'informatica per il giurista*, Giuffrè, Milano, 1990.

L'ultimo spunto di riflessione è dedicato alla *cybersecurity*, dato che la vulnerabilità è aumentata a causa degli effetti dei *cyber attacks*, producendo conseguenze non più circoscritte ai soli sistemi, ma tali da condizionare le scelte dei guidatori.

L'obiettivo della sicurezza informatica è l'individuazione delle strategie migliori per la protezione della dimensione digitale, proteggendola dalle minacce informatiche[57]. Tuttavia, essa non può – né dovrebbe – essere intesa come se fosse una competenza squisitamente tecnica, bensì deve guardare con attenzione all'approccio olistico[58], collocando al centro delle sue attività la protezione degli utenti dalle insidie degli attacchi informatici[59].

Le brevi osservazioni sulla categoria analitico-descrittiva del *müssen* indotto restituiscono i tratti di un dispositivo di condizionamento dell'agire da cui i guidatori dovrebbero essere al corrente. Ciò è possibile solo se viene coltivata la cultura della sicurezza informatica[60]. Il suggerimento è quello di interpretare la *cybersecurity* come una filosofia del diritto: sicurezza, tutela e libertà devono essere i principi cardine[61], facendo emergere negli utenti la consapevolezza delle asimmetrie informative che strutturano le interazioni utenti-sistemi.

Sicuramente l'opzione migliore di difesa dal *müssen* indotto è lo sviluppo delle capacità critiche degli utilizzatori, evitando di affidarsi ciecamente agli *output* dei sistemi.

In conclusione, gli spunti di riflessione propongono di stabilire un quadro rispettoso delle innovazioni tecnologiche, in armonia con la «natura teleologicamente orientata alla realizzazione del sé»[62] a favore degli utenti.

Così, sarà possibile preservare la funzione di ottimizzazione delle tecnologie nelle attività del *démos*, scongiurando i rischi delle forme di condizionamento dell'agire indotto.

Bibliografia

Amato Mangiameli A.C., *Stati post-moderni e diritto dei popoli*, Giappichelli, Torino, 2004.

Amato Mangiameli A.C. – Saraceni G. (a cura di), *Cento e una voce di informatica giuridica*, Giappichelli, Torino, 2023.

Appiah K.A., *Experiments in Ethics*, Harvard University Press, 2008.

Ballarini A., *Diritti interessi ermeneutica*, Giappichelli, Torino, 2012.

Bernardini M.G. – Casalini B. – Giolo O. – Re L. (a cura di), *Vulnerabilità: etica, politica, diritto*, IF Press, Morolo, 2018.

Blengino C. – Mondino S., *Smart cities and smart citizens*: *trasformazioni e rappresentazioni della sicurezza nell'era della dataveglianza*, in R. Brighi – S. Zullo (a cura di), *Filosofia del diritto e nuove tecnologie. Prospettive di ricerca tra teoria e prassi*, Aracne, Roma, 2015, pp. 41-56.

57. S. Pietropaoli, *Informatica criminale. Diritto e sicurezza nell'era digitale. Aggiornata alla legge 90/2024*, Giappichelli, Torino, 2025, pp. 103-104.

58. P.G. Chiara, *L'evoluzione del governo della cybersicurezza: un approccio olistico*, in Th. Casadei – V. Barone – B. Rossi (a cura di), op. cit., pp. 31-44.

59. Nella letteratura scientifica sono state proposte soluzioni empiriche per la *governance* della *cybersecurity*. A questo proposito, è stata suggerita l'adozione di uno "Scudo Giuridico Adattivo": una metodologia che armonizza il quadro normativo in materia di sicurezza informatica, garantendo un sistema conforme sia ai diritti fondamentali degli utenti sia ai requisiti normativi della cibersicurezza. Si rinvia per l'eccellente analisi a M. Farina, *Cibersicurezza e diritti fondamentali, verificabilità, tracciabilità e resilienza normativa*, in Id. (a cura di), *Lo "Scudo Giuridico Adattivo". Intelligenza artificiale, cybersecurity e diritti fondamentali nell'ecosistema SERICS*, Giappichelli, Torino, 2026, pp. 3-44.

60. Come giustamente osservato da Tina Sever e Giuseppe Contissa, per la totale automazione dei veicoli sono da puntellare questi aspetti: la protezione dai dati personali; la tutela contro gli accessi non autorizzati; la sicurezza informatica. Per la completa indagine e le criticità irrisolte si rimanda a T. Sever – G. Contissa, *Automated driving regulations – where are we now?*, in *Transportation Research Interdisciplinary Perspectives*, 24, 2024 pp. 1-19.

61. Cfr. P. Heritier, *Il dilemma della Cybersecurity, tra reale e virtuale: uno sguardo prospettico. Una postfazione*, in *Teoria e critica della regolazione sociale*, 1, 2025, pp. 201-209.

62. L. Palazzani, *Il concetto di persona tra bioetica e diritto*, Giappichelli, Torino, 1996, p. 257.

Borruso R., *L'informatica per il giurista*, Giuffrè, Milano, 1990.

Brighi R. – Zullo S. (a cura di), *Filosofia del diritto e nuove tecnologie. Prospettive di ricerca tra teoria e prassi*, Aracne, Roma, 2015.

Brighi R., *Cybersecurity. Scenari tecnologici e regolamentazione di un'area in espansione*, in T. Casadei – S. Pietropaoli (a cura di), *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, Wolters Kluwer, Milano, 2024, pp. 75-86.

Brighi R. – Ferrari V., *(Cyber)sicurezza e infanzia digitale. Oltre la protezione, verso un uso critico e consapevole della tecnologia*, in T. Casadei – V. Barone – B. Rossi (a cura di), *Giovani in rete. Guida per un uso consapevole delle tecnologie*, Giappichelli, Torino, 2025, pp. 15-30.

Brownsword R., *Law 3.0. Rules and Technology*, Routledge, Abingdon, 2021.

Calo R., *Robotics and the Lessons of Cyberlaw*, in *California Law Review*, 103, 2015, pp. 513-564.

Campagnoli M.N. – Farina M., *Identità digitale e intelligenza artificiale: tra regolazione, poteri asimmetrici e sfide per il futuro*, in *Journal of Ethics and Legal Technologies*, Vol. 7, 1, 2025, pp. 81-115.

Casa F. – Gaetano S. – Pascali G. (a cura di), *Dignità umana nell'era dell'intelligenza artificiale*, il Mulino, Bologna, 2025.

Casadei Th. – Pietropaoli S. (a cura di), *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, Wolters Kluwer, Milano, 2024.

Casadei Th., *Rights in the age of data*, in F. Pedrini (ed.), *Law in the age of Digitalization*, Aranzadi, Madrid, 2024, pp. 45-64.

Casadei T. – Barone V. – Rossi B. (a cura di), *Giovani in rete. Guida per un uso consapevole delle tecnologie*, Giappichelli, Torino, 2025.

Cassano G. – V. Colarocco V. – Gallus G.B. – Micozzi F.P. (a cura di), *Il processo di adeguamento al GDPR europeo. Aggiornato al D. lgs 10 agosto 2018*, Giuffrè, Milano, 2018.

Catanzariti M., *Etica "artificiale": un modello regolatorio*, in *Ars Interpretandi*, 1, 2021, pp. 165-179.

Cavoukian A., *Privacy by design*, IPC Publications, Ottawa, 2009.

Chen J., *Comparison and Optimization of DSRC and C-V2X Technologies: Current Status, Challenges and Future Prospects*, in *Academic Journal of Science and Technology*, Vol. 13, 2, 2024, pp. 42-50.

Chiara P.G., *L'evoluzione del governo della cybersicurezza: un approccio olistico*, in T. Casadei – V. Barone – B. Rossi (a cura di), *Giovani in rete. Guida per un uso consapevole delle tecnologie*, Giappichelli, Torino, 2025, pp. 31-44.

Chiodo S. – Schiaffonati V. (eds.), *Italian Philosophy of Technology. Socio-Cultural, Legal Scientific and Aesthetic. Perspectives on Technology*, Springer, Cham, 2021.

Clarke R., *Information technology and dataveillance*, in *Communication of the ACM*, Vol. 31, 5, 1988, p. 498-512.

Contissa G. – Lagioia F. – Sartor G., *Liability and automation: legal issues in autonomous cars*, in *Network Industries Quarterly*, Vol. 20, 2, 2018, pp. 21-26.

Contissa G. – Godano F. – Sartor G., *Computation, Cybernetics and the Law at the Origins of Legal Informatics*, in S. Chiodo – V. Schiaffonati (eds.), *Italian Philosophy of Technology. Socio-Cultural, Legal Scientific and Aesthetic. Perspectives on Technology*, Springer, Cham, 2021, pp. 91-110.

Contissa G. – Sartor G., *Liability and automation in socio- technical systems*, in B. Wagner – M.C. Ketteman – K. Vieth-Diltmann – S. Montgomery (eds.), *Handbook on Human Rights and Digital Technology. Global Politics, Law and International Relations*, Elgar, Cheltenham-Northampton, 2025, pp. 222-242.

Corso L., *Breve tassonomia dei rapporti fra Intelligenza Artificiale e diritto. Tre questioni*, in *AI Law. International review of Artificial Intelligence*, 2, 2025, pp. 204-222.

Costantini F. – Thomopoulos N. – Steibel F. – Curi A. – Lugano G. – Kovacikova T., *Autonomous vehicles in a GDPR era*: *An international comparison*, in *Advanced in Transport Policy and Planning*, Vol. 5, 2020, pp. 192-213.

Denardis L., *Internet in ogni cosa. Libertà, sicurezza e privacy nell'era degli oggetti iperconnessi*, Luiss, University Press, Roma, 2021.

Di Giandomenico A. – Diodati C. – Ricci F., *Vulnerabilità come risorsa e valorizzazione. Profili giuridici, sociologici ed etico-politici*, Mimesis, Milano-Udine, 2021.

Di Giandomenico A. (a cura di), *Etsi Deus non daretur … Scritti in memoria di Serenella Armellini*, Giappichelli, Torino, 2023.

El Zorkany M. – Yasser A. – Galal A.I., *Vehicle to Vehicle "V2V" Communication: Scope, Importance, Challenges Directions and Future*, in *The Open Transportation Journal*, 14, 2020, pp. 86-98.

ENISA, *Identifying Emerging Cyber Security Threats and Challenges for 2030*, Heraklion, 2023.

ENISA, *ENISA Threat Landscape 2024*, Heraklion, 2024.

Faini F., *Big data e Internet of Things: data protection e data governance alla luce del regolamento europeo*, *in* G. Cassano – V. Colarocco – G.B. Gallus – F.P. Micozzi (a cura di), *Il processo di adeguamento al GDPR europeo. Aggiornato al D. lgs 10 agosto 2018*, Giuffrè, Milano, 2018, pp. 259-280.

Farina M, *Il cloud computing in ambito sanitario tra security e privacy*, Giuffrè, Milano, 2019.

Farina M., *Lo "Scudo Giuridico Adattivo". Intelligenza artificiale, cybersecurity e diritti fondamentali nell'ecosistema SERICS*, Giappichelli, Torino, 2026.

Farina M., *Cibersicurezza e diritti fondamentali, verificabilità, tracciabilità e resilienza normativa*, in Id. (a cura di), *Lo "Scudo Giuridico Adattivo". Intelligenza Artificiale, cybersecurity e diritti fondamentali nell'ecosistema SERICS*, Giappichelli, Torino, 2026, pp. 3-44.

Ferrarese M.R., *Scrittura digitale e normatività tecnologica*, in *Quaderni costituzionali*, 1, 2026, pp. 65-82.

Fioriglio G., *Vulnerabilità aumentata. Diritto, cura e algoritmi nell'era della salute digitale*, Mucchi Editore, Modena, 2025.

Fioriglio G., *Trattamento dei dati sanitari e ricerca medica: profili informatico-giuridici e istituzionali nel contesto europeo*, in *Jura Gentium*, 2, 2025, pp. 1-30.

Floridi L. (ed.), *The Routledge Handbook of Philosophy of Information*, Abingdon, 2016

Furia A. – Zullo S. (a cura di), *La vulnerabilità come metodo. Percorsi di ricerca tra pensiero politico, diritto ed etica*, Carocci, Roma, 2020.

Gazzolo T., *Essere/dover essere. Saggio su Hans Kelsen*, FrancoAngeli, Milano, 2016.

Gazzolo T., *Che cos'è la forza della legge?*, in *Diritto pubblico*, 3, 2023, pp. 861-891.

Gehlen A., *L'uomo nell'era della tecnica. Problemi socio-psicologici della civiltà industriale*, trad. it., SugarCo, Milano, 1967.

Giolo O. – Pastore B. (a cura di), *Vulnerabilità. Analisi multidisciplinare di un concetto*, Carocci, Roma, 2018.

Giolo O., *Il diritto neoliberale*, Jovene, Napoli, 2020.

Gometz G., *L'incertezza del diritto*, Giappichelli, Torino, 2024.

Gutwirth S. – Leenes R. – de Hert P. – Poullet Y. (eds.), *European Data Protection: In Good Health?*, Springer, Cham, 2012.

Heritier P., *Il dilemma della Cybersecurity, tra reale e virtuale: uno sguardo prospettico. Una postfazione*, in *Teoria e critica della regolazione sociale*, 1, 2025, pp. 201-209.

Hildebrandt M. – van den Berg B. (eds.), *Information, Freedom and Property. The philosophy of law meets the philosophy of technology*, Routledge, Abingdon, 2016.

Jaspers K., *La fede filosofica di fronte alla rivelazione*, trad. it., Longanesi, Milano, 1970.

Jonas H., *Dalla fede antica all'uomo tecnologico* (1974), trad. it., il Mulino, Bologna, 1991.

Kelsen H., *Teoria generale delle norme* (1979), a cura di M.G. Losano, Einaudi, Torino, 1985.

Kelsen H., *Che cos'è la dottrina pura del diritto?*, a cura di T. Gazzolo, La nave di Teseo, Milano, 2022.

Kim S. – Shrestha R., *Automotive Cyber Security. Introduction, Challenges and Standardization*, Springer, Cham, 2020, pp. 67-96.

Leenes R. – van Brakel R. – Gutwirth S. – de Hert P. (eds.), *Data Protection and Privacy: (In)visibilities and Infrastructure*, Springer, Cham, 2017

Lyon D., *L'occhio elettronico. Privacy e filosofia della sorveglianza*, trad. it., Feltrinelli, Milano, 1997.

Lyu F. – Li M. – Shen X., *Networking for Road Safety*, Springer, Cham, 2020.

Maceratini A., *Dall'Internet of Things alle Smart Roads. Riflessioni informatico-giuridiche su strade intelligenti, veicoli automatici e connessi*, in *Rivista elettronica di Diritto, Economia, Management*, 3, 2019, pp. 71-91.

Magaia N. – Mastrorakis G. – Mavromoustakis G. – Pallis E. – Markakis E.K. (eds.), *Intelligent Technology for Internet of Vehicles*, Springer, Cham, 2021.

Mancarella M. (a cura di), *Lineamenti di informatica giuridica*, Tangram, Trento, 2024.

Martoni M., *Un'autonomia ostacolata. Limiti cognitivi, incompetenze e design ingannevoli nella trasformazione digitale*, in *Sociologia del diritto*, Vol. 51, 1, 2024, pp. 7-32.

Miniscalco N., *L'Intelligenza Artificiale in movimento. L'impatto sui diritti costituzionali della smart mobility*, Wolters Kluwer, Milano, 2024.

Miucic R. (ed.), *Connected Vehicles. Intelligent Transportation Systems*, Springer, Cham, 2019.

Nissenbaum H.F., *Privacy in context: technology, policy, and the integrity of social life*, Stanford University Press, Redwood City, 2009.

Orecchia R. (a cura di), *La responsabilità politica, diritto, tempo. Atti del XIII Congresso Nazionale* (*Pavia-Salice Terme 28-31 maggio 1981*), Giuffrè, Milano, 1982.

Pagallo U., *Prolegomeni d'informatica giuridica*, Cedam, Padova, 2003.

Pagallo U., *Privacy e design*, in *Informatica e diritto*, Vol. XVIII, 1, 2009, pp. 123-134.

Pagallo U., *On the Principle of Privacy by Design and its Limits: Technology, Ethics and Rule of Law*, in S. Gutwirth – R. Leenes, P. de Hert – Y. Poullet (eds.), *European Data Protection: In Good Health?*, Springer, Cham, 2012, pp. 331-346.

Pagallo U. – Durante M., *The Philosophy of Law in an Information Society*, in L. Floridi (ed.), *The Routledge Handbook of Philosophy of Information*, Abingdon, 2016, pp. 396-407.

Pagallo U. – Durante M. – Monteleone S., *What is new with the Internet of Things in Privacy and data protection? Four legal challenges on sharing and control in IoT*, in R. Leenes – R. van Brakel – S. Gutwirth – P. de Hert (eds.), *Data Protection and Privacy: (In)visibilities and Infrastructure*, Springer, Cham, 2017, pp. 59-78.

Palazzani L., *Il concetto di persona tra bioetica e diritto*, Giappichelli, Torino, 1996.

Palladino A., *Sharing, Data and Smart Mobility. Towards Innovative Urban Paradigms*, Key Editore, Milano, 2024.

Paseri L., *Il governo dei dati. Interesse pubblico, altruismo e partecipazione*, Giappichelli, Torino, 2025.

Pattaro E., *Filosofia del diritto. Diritto. Scienza giuridica* (1978), a cura di M. La Torre, Rubbettino, Soveria Mannelli, 2023

Pedrini F. (ed.), *Law in the age of Digitalization*, Aranzadi, Madrid, 2024.

Perri P., *Sorveglianza elettronica, diritti fondamentali ed evoluzione tecnologica*, Giuffrè, Milano, 2020.

Pettit P., *Il repubblicanesimo* (1977), trad. it., Feltrinelli, Milano, 2000.

Pietropaoli S., *Informatica criminale. Diritto e sicurezza nell'era digitale. Aggiornata alla legge 90/2024 e alla direttiva NIS2*, Giappichelli, Torino, 2025.

Pizzetti F., *Privacy e il diritto europeo alla protezione dei dati personali. Dalla direttiva 95/46 al nuovo Regolamento europeo*, Giappichelli, Torino, 2016.

Pollicino F. – Stabili D. – Marchetti M., *On the effectiveness of BSM communication in V2V emergency scenarios*, in *IEEE 95th Vehicular Technology Conference*, Helsinki, 2022, pp. 1-5.

Kowalski R., *Legislation as Logic Programs*, Imperial College, London, 1991.

Punzi A., *"Accolse l'uomo come opera di natura indefinita". Note su esperienza giuridica e nuovo ordine delle intelligenze*, in *Rivista di filosofia del diritto*, 1, 2025, pp. 21-32.

Rayes A. – Salam S., *Internet of Things. From Hype to Reality*, Springer, Cham, 2017.

Romano B., *Opera Omnia. Ragione sufficiente e diritto. Dataismo e teoria dei quanti*, Giappichelli, Torino, 2023.

Romeo F., *Il dato digitale e la natura delle cose*, in A. Ballarini (a cura di), *Diritti interessi ermeneutica*, Giappichelli, Torino, 2012, pp. 87-124.

Ross A., *Colpa, responsabilità e pena* (1970), trad. it., Giuffrè, Milano, 1982.

Sarra C., *Dignità umana nell'era dell'intelligenza artificiale e della datificazione*, Kront, Roma, 2025.

Sarra C., *L'uomo dato. Antropologia (giuridica) della datificazione*, in F. Casa – S. Gaetano – G. Pascali (a cura di), *Dignità umana nell'era dell'intelligenza artificiale*, il Mulino, Bologna, 2025, p. 157-167.

Sartor G., *Linguaggio giuridico e linguaggi di programmazione*, Clueb, Bologna, 1992.

Scarpelli U., *La responsabilità politica*, in R. Orecchia (a cura di), *La responsabilità politica, diritto, tempo. Atti del XIII Congresso Nazionale* (*Pavia-Salice Terme 28-31 maggio 1981*), Giuffrè, Milano, 1982, pp. 43-95.

Schauer F., *La forza del diritto* (2015), trad. it., Mimesis, Milano-Udine, 2016.

Serra T., *Vulnerabilità e etica della cura*, in A. Di Giandomenico (a cura di), *Etsi Deus non daretur … Scritti in memoria di Serenella Armellini*, Giappichelli, Torino, 2023, pp. 459-466.

Sever T. – Contissa G., *Automated driving regulations – where are we now?*, in *Transportation Research Interdisciplinary Perspectives*, 24, 2024, pp. 1-19.

Shrivastava S., *V2V Vehicle Safety Communication*, in R. Miucic (ed.), *Connected Vehicles. Intelligent Transportation Systems*, Springer, Cham, 2019, pp. 117-155.

Smith C., *The Car Hacker's Handbook. A Guide for the Penetration Tester*, No Starch Press, San Francisco, 2016.

Susco E., *IoT*, in A.C. Amato Mangiameli – G. Saraceni (a cura di), *Cento e una voce di informatica giuridica*, Giappichelli, Torino, 2023, pp. 292-296.

Tincani P., *Sorveglianza e potere. Disavventure dell'asimmetria cognitiva*, in *Ragion pratica*, 1, 2018, pp. 51-78.

Wagner B. – Ketteman M.C. – Vieth-Diltmann K. – Montgomery S. (eds.), *Handbook on Human Rights and Digital Technology. Global Politics, Law and International Relations*, Elgar, Cheltenham-Northampton, 2025.

Yogha K.B., *A Study of V2V Communication on VANET: Characteristic, Challenges and Research Trends*, in *JISA (Jurnal Informatika dan Sains)*, Vol. 4, 1, 2020, pp. 46-58.

Zanetti Gf., *Equality and Vulnerability in the Context of Italian Political Philosophy. Italian Efficacy*, Springer, Cham, 2023.

Ziccardi G., *Diritti digitali. Informatica giuridica per le nuove professioni*, Raffaello Cortina Editore, Milano, 2022.