Carla Maria Saracino

Cybersecurity e mobilità intelligente: il binomio sicurezza/responsabilità

Abstract: Lo stato dell'arte europeo in ordine ai sistemi di trasporto intelligente risente delle diverse velocità di adeguamento degli Stati alle Direttive e agli atti di programmazione europei e dalla diversa sensibilità al fenomeno della mobilità sicura, digitale ed eco-integrata. Trattandosi di un tema che, inevitabilmente, coinvolge gli ambiti del diritto della sicurezza, dell'innovazione e dell'ambiente, lo studio si propone di indagarne tre aspetti fondamentali: la necessità di una regolamentazione del settore che necessita di una regolamentazione puntuale, di parametri applicativi e coordinate chiare; il connubio tra sicurezza individuale e appalti per l'innovazione, nelle forme del partenariato per l'innovazione e dei contratti di ricerca e sviluppo; la regolamentazione dei profili di responsabilità connessi, nonché la tutela dei *big data* e degli algoritmi che supportano i sistemi di mobilità sostenibili. In tali ambiti, avrà senso indagare l'atteggiarsi del potere regolatorio pubblico in relazione alle fattispecie di trasporto automatizzato.

Keywords: Mobilità intelligente; Innovazione; Cybersicurezza; Regolazione; Responsabilità.

1. Premessa

Lo stato dell'arte europeo in ordine ai sistemi di trasporto intelligente risente delle diverse velocità di adeguamento degli Stati alle Direttive e agli atti di programmazione europei e dalla diversa sensibilità al fenomeno della mobilità sicura, digitale ed eco-integrata. Trattandosi di un tema che, inevitabilmente, coinvolge gli ambiti del diritto della sicurezza, dell'innovazione e dell'ambiente, ci si propone di indagarne tre aspetti fondamentali.

In primo luogo, la disamina intenderà soffermarsi sulla necessità di una regolamentazione t*ough* del settore che necessita, più che di raccomandazioni e linee guida non vincolanti ascrivibili nel *soft law*, di una regolamentazione puntuale, di parametri applicativi e coordinate chiare per l'introduzione e, poi, la gestione di fenomeni di guida automatizzata e di trasporto digitale. In particolare, ci si propone

Teoria e Critica della Regolazione Sociale, n. 1, 2025 • Mimesis Edizioni, Milano-Udine Web: www.mimesisjournals.com/ojs/index.php/tcrs • ISSN (online): 1970-5476 • ISBN: 9791222320793 • DOI: 10.7413/197054760165
© 2025 – MIM EDIZIONI SRL. This is an open access article distributed under the terms of the Creative Commons Attribution License (CC-BY-4.0).

di analizzare la regolamentazione relativa alla sperimentazione su strada pubblica dei veicoli a guida autonoma nel contesto italiano, alla luce del c.d. Decreto *Smart Roads* e dei connessi problemi di *cybersecurity,* soffermandosi, in particolare, sulla vigilanza del funzionamento del sistema automatico.

In secondo luogo, l'indagine sarà rivolta a considerare il connubio tra sicurezza individuale e appalti per l'innovazione, nelle forme del partenariato per l'innovazione e dei contratti di ricerca e sviluppo per l'approdo a soluzioni di trasporto automatizzato ed eco-sostenibile e la tutela degli eco-sistemi.

In tale prospettiva, occorre considerare l'intreccio tra tecnologie informatiche, *software* applicativi e *start up* promotrici di processi di accertamento delle violazioni stradali e dell'ampliamento di soluzioni per la digitalizzazione.

Ci si propone di considerare una necessaria sinergia tra il sistema del *green procurement*[1] e la possibile progettazione di soluzioni non ancora presenti sul mercato che riducano i rischi di esternalità negative e progettino soluzioni di trasporto autonomo in applicazione del principio *security by design* (sicurezza durante la progettazione e sviluppo) che richiede competenza degli attori coinvolti in materia di *cybersecurity*.

Infine, aspetto centrale e connesso agli aspetti già tratteggiati, attiene alla regolamentazione dei *big data* e degli algoritmi che supportano i sistemi di mobilità sostenibile e sono in rapporto di intersezione con la riservatezza degli utenti.

In tale ambito, avrà senso indagare il diverso atteggiarsi del potere conoscitivo pubblico in relazione alle fattispecie di trasporto automatizzato e digitalizzato e alle procedure algoritmiche che ne sono alla base.

Riflettere sulla necessità di un archivio tutelato di dati assume importanza, ove si considerino le prospettive di ampliamento del fenomeno e la sua progressiva diffusione, valorizzando, così, *de iure condendo,* i poteri di organizzazione dell'ENISA e delle Autorità nazionali di Cybersicurezza.

Il *fil rouge* della trattazione pare riconducibile ai due poli fondamentali della sicurezza e della responsabilità, declinati nel settore della cybersicurezza e dell'introduzione/diffusione di modelli di mobilità intelligente nei contesti delle *smart cities* e delle politiche dei trasporti per le future generazioni.

Il tema investe le dinamiche partecipative dei privati ai processi decisori pubblici, ma involge, necessariamente, una riflessione sul ruolo dei pubblici poteri e sulle scelte in ordine alle modalità di *governance* idonee a regolare la complessità delle nuove applicazioni tecnologiche ai contesti socio-economici.

1 La connettività dei veicoli e l'integrazione, all'interno di un sistema, di migliaia di componenti generano minacce di attacchi informatici, come quelle sul controllo a distanza dei veicoli, che vanno regolamentate e affrontate con gli strumenti preventivi del *risk assessment.* La disposizione concernente le misure di sicurezza informatica nel Codice dei contratti pubblici è stata introdotta all'articolo 108, *Criteri di aggiudicazione degli appalti di lavori, servizi e forniture*, comma 4. Tale norma prevede che le stazioni appaltanti tengano sempre in considerazione gli elementi di *cybersicurezza* nell'approvvigionamento di beni e servizi informatici, in particolare quando l'impiego dei suddetti beni e servizi risulti essere connesso alla tutela degli interessi nazionali strategici.

2. Lo stato dell'arte europeo e nazionale in tema di *smart mobilities*

Priorità dell'attuale contesto ordinamentale sono, data l'emergenza ambientale, la riduzione della congestione e dell'inquinamento atmosferico; l'aumento della sicurezza dei trasporti e della sicurezza informatica, il migliore coordinamento tra interventi infrastrutturali e regolamentazione giuridica dell'impatto sociale prodotto dagli stessi.

I sistemi di trasporto intelligente, le reti informatiche, i nodi intermodali e le piattaforme di interoperabilità sono destinati ad assumere un ruolo paradigmatico, considerato che la diffusione di tali sistemi è funzionale al raggiungimento di obiettivi di matrice sociale e di politica economica.

L'implementazione di misure di sicurezza stradale è stata perseguita a livello europeo, ai fini della realizzazione di obiettivi di crescita economica e tutela della qualità della vita, come emerge dagli atti della Commissione europea, ma anche del Paramento dell'Unione e del Comitato economico e sociale europeo.

Nel Libro bianco della Commissione, l'aspetto economico viene anteposto a quello sociale[2] e un tale approccio dell'Unione trova conferma anche nella Proposta di direttiva del Parlamento europeo e del Consiglio che modifica la direttiva 2006/22/CE per quanto riguarda le prescrizioni di applicazione e fissa norme specifiche per quanto riguarda la direttiva 96/71/CE e la direttiva 2014/67/UE sul distacco dei conducenti nel settore del trasporto su strada[3].

Anche il Parlamento europeo, in una recente risoluzione[4], "invita la Commissione ad assicurare che il mercato abbia un tempo sufficiente e realistico per adattarsi a queste misure". A livello nazionale, una prima regolamentazione del fenomeno è stata delineata dal *Decreto Smart Roads*[5] che ha contribuito a definire le *smart roads* come infrastrutture stradali per le quali è stato compiuto un processo di trasformazione digitale orientato a introdurre piattaforme di osservazione e monitoraggio del traffico, nonché modelli di elaborazione dei dati e delle informazioni, nel quadro della creazione di un ecosistema tecnologico favorevole all'interoperabilità tra infrastrutture e veicoli di nuova generazione.

2 "[i] trasporti sono fondamentali per la nostra economia e la nostra società. La mobilità svolge un ruolo vitale per il mercato interno e la qualità di vita dei cittadini che fruiscono della libertà di viaggiare. I trasporti sono funzionali alla crescita economica e dell'occupazione".

3 COM(2017) 278 final, 31 maggio 2017. Inoltre, la Commissione dedica una specifica comunicazione "per illustrare la strategia dell'UE per una diffusione coordinata dei sistemi C-ITS che permetta di evitare la frammentazione del mercato interno in questo settore e di creare sinergie tra le diverse iniziative". Comunicazione della Commissione, Una strategia europea per i sistemi di trasporto intelligenti cooperativi.

4 Parlamento europeo, risoluzione 14 novembre 2017, punto 52. Si v., inoltre, Risoluzione del Parlamento europeo del 18 maggio 2017 *sul trasporto stradale nell'Unione europea*, cit., punto E), nonché punti 1 ss. (in cui si parla di competitività) e 20 ss. (in cui si parla di norme sociali e condizioni di sicurezza).

5 Decreto ministeriale 28 febbraio 2018 attuativo delle numerose disposizioni della Legge di Bilancio 2018 che mirano all'ammodernamento e all'adeguamento tecnologico di tutta la rete stradale italiana all'insegna della *digital tansformation.*

Il processo di trasformazione digitale in fase di sperimentazione è orientato da modelli di gestione e verifica dei dati di progetto, nonché dal monitoraggio di sistemi orientati alla sicurezza strutturale degli elementi che compongono le infrastrutture stradali.

La prima normativa europea volta ad armonizzare le regole in materia di cybersicurezza tra Stati membri è stata la Direttiva NIS 1[6] con l'obiettivo di raggiungere un livello comune ed elevato di resilienza in UE e di innalzare la cooperazione tra gli Stati membri, creando un primo livello di armonizzazione in materia di sicurezza cibernetica.

Essa individua le categorie di soggetti a cui sono rivolte previsioni specifiche e, in particolare, gli operatori di servizi essenziali, caratterizzati come soggetti pubblici o privati che forniscono *utilities* e richiede che gli Stati adottino una strategia nazionale in materia di sicurezza cibernetica, volta a definire obiettivi strategici e priorità, nonché misure di regolamentazione a livello nazionale, volte ad assicurare la cooperazione internazionale e la collaborazione con l'ENISA attraverso meccanismi individuati.

La Direttiva NIS 1 impone, essenzialmente, obblighi e misure di sicurezza adeguate e proporzionate alla gestione dei rischi e alla prevenzione e minimizzazione dell'impatto degli incidenti di sicurezza, nonché misure relative alla segnalazione di incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali prestati. Il quadro normativo delineato dalla Direttiva NIS 1 è stato, successivamente, rafforzato e aggiornato dalla Direttiva NIS 2[7] che ha progressivamente contribuito a eliminare le divergenze tra ordinamenti, rafforzando gli obblighi di *cybersecurity* e ampliando il numero di settori e soggetti coinvolti, nonché aumentando la cooperazione tra gli Stati per raggiungere maggiore uniformità di applicazione.

Tale Direttiva rafforza, sostanzialmente, gli obblighi già presenti all'interno della Direttiva NIS 1, quali, in particolare, le misure di sicurezza operative e organizzative adeguate e proporzionate per gestire i rischi dei sistemi di rete e le informazioni che tali soggetti utilizzano per la fornitura dei loro servizi e per prevenire o ridurre al minimo l'impatto degli incidenti sui destinatari dei loro servizi e su altri servizi.

La Direttiva NIS 2 fornisce un elenco minimo delle misure di sicurezza che devono essere implementate e, ove opportuno, viene prevista la notifica senza indebito ritardo degli incidenti significativi anche nei confronti dei destinatari dei servizi stessi.

A queste previsioni, si aggiungono le prescrizioni rivolte agli Stati membri, circa la necessità di prevedere misure di vigilanza ed esecuzione, nonché nuovi obblighi di condivisione delle informazioni sulla cybersicurezza.

Tale Direttiva, in particolare, ridetermina e amplia l'ambito di applicazione delle norme in materia di sicurezza dei dati e potenzia gli organi e le attività di super-

6 Essa è stata adottata il 6 luglio 2016 e recepita in Italia con il d.lgs. 65/2018 ed è stata, poi, abrogata con l'entrata in vigore della Direttiva NIS 2. La Direttiva NIS 1, acronimo di "*Network and Information Security*", viene adottata nel 2016.

7 La Direttiva UE 2022/2555, adottata il 14 ottobre 2022, dovrà essere recepita nella legislazione nazionale entro il 17 ottobre 2024.

visione a livello comunitario, al fine di razionalizzare i requisiti minimi di sicurezza ed estendere i concetti di gestione del rischio.

Da tale Direttiva scaturisce un sistema di ampliamento delle responsabilità, estesa non più soltanto all'azienda titolare del servizio, ma anche a tutti gli *stakeholder* che intervengono lungo la *supply chain.*

L'obiettivo del legislatore è di espandere la cultura e gli obblighi di sicurezza a tutti gli attori coinvolti, al fine di creare un clima di responsabilità condivisa.

Con riguardo alle nuove competenze professionali richieste ai lavoratori nel settore dell'industria della mobilità derivante dall'impiego maggiore di dispositivi informatici e automatizzati sempre più sofisticati è stato elaborato un quadro di raccomandazioni[8] sulle necessarie basi di un'alfabetizzazione digitale.

Il rischio legato ai dati prodotti dal ricorso alla tecnologia (sistemi di trasporto intelligente, intelligenza artificiale, veicoli automatizzati), non solo con riferimento ai *big data,* ma anche sotto altri profili[9], ha ottenuto regolamentazione, di recente, con una serie di atti delle autorità amministrative indipendenti.

In Italia, l'Autorità garante della concorrenza e del mercato, l'Autorità per le garanzie nelle comunicazioni e il Garante per la protezione dei dati personali hanno avviato[10] un'indagine conoscitiva congiunta, riguardante l'individuazione di eventuali criticità connesse all'uso dei cosiddetti *big data* e la definizione di un quadro di regole in grado di promuovere e tutelare la protezione dei dati personali[11], la

8 Si veda, sul punto, comunicazione della Commissione, *L'Europa in movimento. Un'agenda per una transizione socialmente equa*, nonché CESE su *Il ruolo dei trasporti nella realizzazione degli obiettivi di sviluppo sostenibile.* Sulla nozione di guida autonoma si vedano Battistella 2021: 953; Salerno 2019.

9 Secondo la definizione elaborata dalla Commissione europea (*Digital single market – Big Data,* disponibile alla pagina web https://ec.europa.eu/digital-single-market/en/big-data), "*[b]ig data refers to large amounts of data produced very quickly by a high number of diverse sources. Data can either be created by people or generated by machines, such as sensors gathering climate information, satellite imagery, digital pictures and videos, purchase transaction records, GPS signals, etc. It covers many sectors, from healthcare to transport and energy*". Sui *big data* in generale si veda OECD, *Data driven innovation. Big data for growth and well-being*, October 2015

10 In data 30 maggio 2017, l'Autorità Garante della Concorrenza e del Mercato, l'Autorità per le Garanzie nelle Comunicazioni e il Garante per la protezione dei dati personali hanno avviato congiuntamente un'Indagine Conoscitiva per meglio comprendere le implicazioni per la privacy, la regolazione, la tutela del consumatore e l'antitrust, dello sviluppo dell'economia digitale e, in particolare, del fenomeno dei *Big Data.*

11 In data 13 marzo 2018 il Parlamento europeo A8-0036/18/ P8_TA – PROV(2018)0063) ha elaborato uno studio sulla *Strategia europea per i sistemi di trasporto intelligenti cooperativi*, nella quale il Parlamento europeo ha invitato la Commissione a pubblicare una proposta legislativa che garantisca condizioni di parità per l'accesso ai dati e alle risorse di bordo dei veicoli, tutelando i diritti dei consumatori e promuovendo l'innovazione e una concorrenza leale. Più in generale sul tema, si veda la comunicazione della Commissione, *Verso uno spazio comune europeo dei dati*, COM(2018) 232, pubblicata il 25 aprile 2018, la quale fornisce orientamenti sulla condivisione di dati tra imprese e tra imprese e pubblica amministrazione, oltre a quelli di cui alla comunicazione della medesima Commissione *Costruire un'economia dei dati europea*, COM (2017) 9 final del 10 gennaio 2017, sull'ubicazione dei dati e i principi guida indicati nella relazione della piattaforma per la diffusione dei sistemi di trasporto intelligenti e cooperativi. Si veda, inoltre, la Proposta di regolamento relativo a un quadro applicabile alla libera circolazione

concorrenza dei mercati dell'economia digitale, la tutela del consumatore a fronte dell'introduzione di sistemi di interoperatività tecnologica nei trasporti.

Al quadro normativo delineato dalle due citate Direttive si è aggiunta, di recente, la regolamentazione ad opera della CER, Direttiva *risk based*[12] che fornisce indicazioni sulla identificazione delle entità critiche, definendo misure minime e procedure comuni per il *reporting* e la cooperazione tra Stati. Tale direttiva fornisce indicazioni sulla identificazione delle entità critiche, definisce le misure minime per raggiungere un grado definito di resilienza e stabilisce procedure comuni per il *reporting* e la cooperazione tra Stati. Inizio modulo

3. Rischio, precauzione e prevenzione: il diritto della paura

Il tema della mobilità digitalizzata e automatizzata, così come attualmente configurata alla luce del quadro europeo e nazionale, interseca i temi fondamentali della sicurezza e della responsabilità.

La sicurezza dei sistemi informatici è da intendersi come nuova rilevante frontiera dell'esercizio del potere amministrativo con funzione di prevenzione.

La rilevanza della connessione tra benessere complessivo e sicurezza emerge dall'art. 3, co. 2 TUE che specifica che "l'Unione offre ai suoi cittadini uno spazio di libertà, sicurezza e giustizia", nonché dall'art. 4 c.2 TUE nella parte in cui precisa il necessario rispetto dell'identità nazionale e delle funzioni dello Stato nel mantenimento dell'ordine pubblico e nella tutela della sicurezza nazionale.

A differenza di un originario sistema fondato su autoritatività e prescrittività, in cui la sicurezza radicava il proprio inveramento nell'esercizio di poteri impositivi, nell'attuale ordinamento costituzionale, tuttavia, trova fondamento il principio di proporzionalità, quale strumento di modulazione dell'intervento dei pubblici poteri.

dei dati non personali, COM (2017) 495 del 13 settembre 2017 che ha l'obiettivo di rimuovere le restrizioni ingiustificate in materia di localizzazione dei dati, rafforzando la libertà delle aziende di archiviare o trattare i propri dati non personali ovunque vogliano all'interno dell'Unione.. FOTINA, *Rete senza regole, ci provano le Autorità*, in *Il Sole 24 Ore* del 26 gennaio 2018. Anche la OECD (*Technology Foresi-ght Forum 2016 on Artificial Intelligence (AI)*, 17 November 2016, consultabile alla pagina web http://www.oecd.org/internet/ieconomy/technology-foresight-forum-2016. htm) osserva come il tema della intelligenza artificiale, in particolare, sia sottovalutato da "*policymakers and the public at large*", soprattutto se si tiene conto della circostanza che "*[i]t is widely claimed that artificial intelligence technology, combined with "big data" and with computing power, will transform entire sectors of the economy and lead to in-depth societal changes*".

12 Tale nuova direttiva sulla resilienza e quindi sulla sicurezza cinetica delle infrastrutture critiche, oggi denominate entità critiche, che sostituisce la direttiva 114/08 sulla identificazione e designazione delle Infrastrutture critiche europee, è stata pubblicata a dicembre 2022 in Gazzetta Ufficiale, insieme con la Direttiva NIS 2 dedicata alla sicurezza *cyber* delle entità critiche e al regolamento DORA sulla sicurezza delle entità del settore finanziario e bancario. Le due direttive emanate all'unisono riconciliano il concetto di sicurezza fisica o cinetica, come si dice oggi, con quello della sicurezza logica o *cyber*. La NIS2 si occupa infatti della sicurezza cyber delle entità critiche e altamente critiche e la CER della loro resilienza rispetto a minacce cinetiche sia naturali che antropiche, volontarie o involontarie, ivi comprese le minacce di stampo terroristico.

L'individuazione della nozione di sicurezza diviene nodo problematico, trattandosi di una nozione sfuggente e dai confini incerti, identificata in senso positivo con la nozione di ordine pubblico interno e internazionale.

La parabola definitoria della nozione di sicurezza ha risentito, nel corso dei differenti periodi storici, delle diverse concezioni di ordine pubblico delineate e del differente peso dell'intervento dello Stato sulla sfera giuridica dei cittadini.

L'ampio concetto della funzione di polizia di sicurezza enucleato agli inizi del '900 è stato ricostruito riconducendo ad essa poteri generali di prevenzione idonei anche a comprimere la libertà personale, qualora essa sia tale da costituire minaccia per l'ordine pubblico e la sicurezza generale dei cittadini.

Le articolazioni e le esplicazioni della polizia di sicurezza erano individuabili nell'osservazione, nella prevenzione e nella repressione, al fine di impedire le violazioni dell'ordine giuridico.

Lo sviluppo dei poteri di polizia e prevenzione veniva codificato nei Testi Unici di pubblica sicurezza e introduceva un concetto di ordine pubblico dilatato, rafforzando gli strumenti finalizzati a evitare che non avvenisse "nulla di nocivo all'ordine e alla sicurezza dello Stato e delle sue parti, perché non si compiano quei fatti che, avvenuti, perturberebbero l'interesse pubblico e il privato"[13].

Anche dopo l'avvento della Costituzione si è riscontrato l'espandersi di tale tutela sul piano della sicurezza interna ed internazionale, identificando la funzione del sistema di sicurezza pubblica con una funzione negativa di conservazione dell'ordine pubblico, in termini di rimozione delle turbative prevenzione dei pericoli.

Alla base della concezione tradizionale della sicurezza, preservata tramite poteri di polizia e strumenti di prevenzione e fondata sul principio di proporzionalità, vi è il concetto di pericolo, riscontrato qualora una determinata circostanza di fatto origini una sequenza causale che, con certezza scientifica o con probabilità vicina alla certezza, condurrà alla determinazione di un danno.

Nella dogmatica successiva è stata attuata una sorta di superamento del concetto di pericolo, risultando, invece, valorizzato il concetto di tutela precauzionale a fronte dell'esistenza di rischi potenziali che attentino non solo ad aspetti materiali attinenti all'incolumità e alla sanità, ma anche ad un ordine pubblico ideale inteso in senso dinamico e comprensivo di istanze economiche e sociali[14].

Tale concezione ha preso le mosse dal concetto di rischio, inteso come danno potenziale in condizioni di incertezza causale, idoneo a determinare l'emergere di un'amministrazione del rischio, fondata sulla valorizzazione del principio di precauzione.

Nell'attuale realtà ordinamentale italiana è riscontrabile, tuttavia, una progressiva sovrapposizione tra pericolo e rischio[15], tra prevenzione e precauzione e un'evoluzione verso un sistema di tutele in cui risultino integrati i poteri di polizia intesi in senso preventivo e gli atti di *soft law*.

13 Si v. Ranelletti 1904: 216.
14 Si v. Paladin 1965: 130; Cerri 2007: 2.
15 Barone 2020: 63-68.

A tal proposito, è d'uopo rilevare come si assista a un passaggio da un diritto dell'emergenza a un diritto del rischio che tende a sfumare nella nozione di pericolo.

Si verifica una sorta di sovrapposizione tra precauzione e prevenzione. Non essendoci una certezza scientifica sul verificarsi di una determinata serie causale, si tende ad approntare degli strumenti di prevenzione che possano tener conto del bilanciamento di più fattori.

Si tende, pertanto, ad un mutamento dei modelli di regolazione. Se secondo una sfera precauzionale si tende a poteri più ampi, connotati da una regolamentazione dolce, ove si intraveda la sussistenza di una necessaria prevenzione di pericoli, si tende a spostarsi verso una regolazione più vincolante, rigida che pone parametri prescrittivi che vanno verso la sanzione e che tendano alla conformazione.

In tale contesto, alla luce della sempre maggiore rilevanza di strumenti preventivi, emerge la necessità di coordinate di regolamentazione chiare, supportate da valutazioni tecniche e temperate dal principio di proporzionalità[16].

4. La sicurezza nazionale cibernetica e la moltiplicazione dei nessi di causalità

Un'articolazione definitoria della nozione di sicurezza, così come delineata anche alla luce del nuovo complesso sistema ordinamentale, è costituita dalla *cybersicurezza*, intesa come capacità di resistere a ogni azione che comprometta la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati o trasmessi in relazione ai servizi offerti o accessibili tramite tale rete o altri sistemi informativi, nonché di impedire ogni azione diretta a ostacolare il funzionamento del sistema tecnologico.[17]

In particolare l'ambito della sicurezza viene declinato, con riferimento ai sistemi di trasporto intelligente, sia come sicurezza individuale, caratterizzata da strumenti di prevenzione utilizzati al fine di realizzare gli obiettivi pertinenti alla riduzione dei fenomeni di sinistri stradali che a livello di sicurezza cibernetica, intesa con riguardo all'impedimento di attacchi informatici tali da impedire il funzionamento dei sistemi di *smart mobilities.*

La sicurezza nazionale cibernetica si configura, pertanto, come una nuova frontiera dell'esercizio del potere amministrativo con funzione di prevenzione ed è regolata dal Regolamento UE 2019/881 (*Cybersecurity act)* che prevede un inse-

16 De Nitto 2023. La Comunicazione della Commissione, *Verso uno spazio europeo della sicurezza stradale*, specifica che gli orientamenti europei per la sicurezza stradale riguardano l'orizzonte temporale fino al 2020 e "intendono definire un quadro di governance generale e obiettivi ambiziosi che servano a orientare le strategie nazionali o locali". Una posizione simile a quella espressa dalla Commissione si rinviene nella risoluzione del Parlamento europeo del 27 settembre 2011 sulla sicurezza stradale in Europa 2011-2020, punto 2, nonché più recentemente, nella prospettiva dell'economia collaborativa, nella risoluzione del Parlamento europeo del 15 giugno 2017 su un'agenda europea per l'economia collaborativa.

17 Art. 4 n. 2 direttiva NIS.

rimento di soggetti pubblici e privati nel perimetro della cybersicurezza al fine di regolamentare i fenomeni di digitalizzazione e i circuiti *blockchain*[18] estesi alle filiere produttive e al settore dei trasporti.

La diffusione di modelli di digitalizzazione nel settore della mobilità ha imposto, contestualmente all'accelerazione dei processi e alla semplificazione dei procedimenti, problemi di responsabilità. Nell'ambito dei veicoli a motore, i problemi di responsabilità già gravosi con riferimento ai nessi di causalità, da riscontrare in materia di sinistri stradali, divengono molteplici nel settore della regolamentazione per la guida autonoma e per il trasporto automatizzato e intelligente.

I problemi tradizionali di responsabilità sono affrontati, a livello di legislazione dell'Unione, da diverse fonti, come la direttiva sull'assicurazione degli autoveicoli[19] e la direttiva sulla responsabilità dei prodotti che trovano recepimento nel contesto nazionale con la delineazione dei diversi regimi di responsabilità degli Stati membri.

In ordine al risarcimento delle vittime, la direttiva sull'assicurazione degli autoveicoli prevede già il risarcimento tempestivo delle vittime degli incidenti causati dai veicoli. La diffusione di modelli di mobilità intelligente ha determinato una effettiva moltiplicazione dei nessi causali e un necessario affinamento dei paradigmi di interpretazione dei processi di causazione. All'introduzione di nuovi meccanismi di funzionamento seguono plurimi indici di rischio, per cui si verifica una proliferazione dei nessi causali e dei profili di responsabilità.

L'introduzione di gestioni *automotive* e circuiti automatizzati di regolazione dei trasporti implica, infatti, un governo degli accadimenti che possano causare un arresto delle funzionalità informatiche, una deviazione dalla processazione algoritmica preindividuata o una indebita ingerenza e/o alterazione dei *big data* inevitabilmente coinvolti nel sistema di gestione digitalizzata dei trasporti.

Nell'interruzione della logica algoritmica diviene problematica l'individuazione della serie causale effettivamente determinativa del danno, nonché dispendioso l'acclaramento eziologico, a fronte dell'effettiva moltiplicazione dei nessi.

In tale prospettiva di progressiva sovrapposizione tra rischio e pericolo e in condizioni di effettiva incertezza epistemico-scientifica emerge uno statuto della causalità fondato su modello probabilistico e controfattuale che diviene maggiormente complesso, tanto più complessa e multistrutturata si configuri la catena dei rapporti eziologici tra gli agenti. Si consideri, inoltre, come tale prospettiva di responsabilità sia contigua al tema della necessaria tutela della riservatezza e della impermeabilità dei dati sensibili inseriti nei sistemi *automotive*, la cui violazione determina profili di illegittimità suscettibili di richiedere una regolamentazione da parte delle autorità nazionali di regolazione.

18 Rubechini 2023; Giardino 2020: 123 ss.

19 Si v la recente direttiva europea 2021/2118, che dal 23 dicembre 2023 obbliga ad assicurare anche i veicoli in sosta in aree private non accessibili al pubblico. Con riferimento alla sicurezza dei prodotti si v. Direttiva (UE) 2019/771 del Parlamento europeo e del Consiglio, del 20 maggio 2019.

5. La necessità di coordinate chiare nel security by design

Dal composito quadro delineato emerge la necessità di un ruolo presente delle istituzioni pubbliche nella regolamentazione[20].

Nella prospettiva indicata, infatti, la realizzazione di obiettivi di sostenibilità e digitalizzazione passa per la definizione *ex ante* della misura della sostenibilità stessa e delle sue modalità attuative sulla base di coordinate prescrittive.

L'auspicio è nell'assunzione da parte dei pubblici poteri di iniziative di regolazione fondate su valutazioni tecniche, fondate sul principio di proporzionalità e mirate all'adozione di coordinate volte a delineare un quadro strategico dell'Unione per la sicurezza stradale per il decennio successivo al 2020 annunciato dal Consiglio, al fine di rafforzare l'ancora debole quadro giuridico dell'Unione in materia di sicurezza stradale e in materia di mobilità autonoma, consentendo la cooperazione non solo a livello intra-UE (tra Stati membri e Unione europea), ma anche a livello internazionale, sotto l'egida delle Nazioni Unite.

Si tratta, per tale via, di assoggettare l'esercizio del potere privato ad alcuni limiti inderogabili finalizzati alla prevenzione e alla neutralizzazione dei rischi di esternalità negative che, nell'epoca della transizione digitale, si sostanziano in ricadute nocive dal punto di vista economico e sociale. Ne deriva che il settore della mobilità intelligente e automatizzata diviene ambito inglobato nel perseguimento di obiettivi di transizione meta-individuali che necessitano, per poter essere realizzati, di un apparato di regole, oltre che di ampie indicazioni di principio. Pare di poter intravedere la necessaria evoluzione verso una necessaria prescrittività della normativa di settore che ridefinisca la dimensione del binomio pericolo/prevenzione e indirizzi il settore della *smart mobilities* verso una regolamentazione idonea a contemperare obiettivi di sicurezza e discernimento di responsabilità.

Bibliografia

Ammannati L. 2018, "Diritto alla mobilità e trasporto sostenibile. Intermodalità e digitalizzazione nel quadro di una politica comune dei trasporti", in *Federalismi.it* (4)1 ss.

Angelini M. 2021, "Metodologia per il cybersecurity assessment con il Framework Nazionale per la Cybersecurity e la Data Protection", in www.framesecuritynetwork.it

Barone A. 2020, "Amministrazione del rischio e intelligenza artificiale", in *European review of digital administratio & law* (1), 63 ss.

Battistella V. 2021, "Spunti di riflessione sulla conduzione dei veicoli altamente automatizzati nella circolazione stradale in una prospettiva de iure condendo", in *Dir. trasp.*, *953*.

Buoso E. 2023, *Potere amministrativo e sicurezza nazionale cibernetica*, Torino: Giappichelli.

Caruso E. 2020, "Trasporto pubblico locale non di linea e mobilità condivisa tra continuità e discontinuità regolativa", in *Politiche e regole per la sharing mobility, Diritto e questioni pubbliche*.

20 Caruso 2020; Ammannati 2018: 1 ss.; Gaspari 2018; Quadri 2017: 39 ss.

Cerri A. 2007, "Ordine pubblico II) Diritto costituzionale. Postilla di aggiornamento" in *Enc. giur.,* XXII, 2.

De Nitto S. 2023, *La proporzionalità nel diritto amministrativo*, Torino: Giappichelli.

Gaspari F. 2018, *Smart city. Agenda urbana multilivello e nuova cittadinanza amministrativa*, Napoli: Editoraile scientifica.

Giani L. 2018, *Dal diritto dell'emergenza al diritto del rischio,* Napoli: Esi.

Giardino E. 2017, "La realizzazione delle infrastrutture di comunicazione elettronica tra poteri statali e veti locali"*,* in *Giustamm.it*.

Montessoro P.L. 2019, "Cybersecurity, conoscenza e consapevolezza come prerequisiti dell'amministrazione digitale", in *Istituzioni del* federalismo, (3), 783.

Paladin L. 1990, "Ordine pubblico, II) Diritto costituzionale", in *Enc. giur.,* XXII, 2.

Quadri S. 2017, "La governance del trasporto pubblico locale in Italia: quali prospettive?" in L. Ammannati, A. Canepa (a cura di), *Politiche per un trasporto sostenibile. Governence, multimodalità e fiscalità,* Napoli: Editoriale Scientifica, 39 ss.

Ranelletti O. 1904, "La polizia di sicurezza", in V.E. Orlando (diretto da), *Primo Trattato completo di diritto amministrativo italiano*, vol. IV, Milano, 216.

Rubechini P. 2023, *Tecnologia, blockchain e fiducia amministrativa*, Napoli: Editoriale scientifica.

Salerno F. 2020, "L'automazione nel trasporto stradale, ferroviario e multimodale", in *Riv. dir. nav.* 94 ss.

Simbula M., Giordano M.T., Oldani I. 2020, "Principi di sicurezza applicabili ai "cloud computing services": GDPR, Direttiva NIS e PSD2 a confornto (Security principles applicable to cloud computing services:comparison between GDPR, NIS Directive and PSD2)", in *Ciberspazio e Diritto* (1) 123 ss.