IAIC MiBACT DGBIC CREDA

Diritto Mercato Tecnologia

15 Giugno 2017

La privacy del guidatore al tempo della mobilità intelligente

Maria Chiara Meneghetti

Nuova Editrice Universitaria

La *privacy* del guidatore al tempo della mobilità intelligente

Maria Chiara Meneghetti

Abstract

Il futuro della mobilità sarà sempre più intelligente. Dai *connected vehicle* agli *autonomous vehicle* il passo è breve. Nella corsa alla digitalizzazione, anche l'Europa si è mossa in questa direzione istituendo una piattaforma di confronto e dialogo per i numerosi attori coinvolti nella realizzazione del progetto: la C-ITS *Platform.* L'obbiettivo è l'inaugurazione del primo sistema di trasporto connesso e intelligente a livello europeo entro il 2019. Un obbiettivo, che deve confrontarsi con le difficoltà tecniche e giuridiche legate alla sua effettiva implementazione. La valutazione dell'impatto che il nuovo sistema produrrà sul diritto alla *privacy* e protezione dei dati dei moderni guidatori è tra le questioni più complesse.

Abstract

The future of mobility will become increasingly smart. Connected vehicles are only few steps away from autonomous vehicles. In the rush to digitalization, also Europe has moved in this direction establishing a platform of discussion and dialogue among the multiple actors involved in the deployment of the project: the C-ITS Platform. The objective is the inauguration of the first connected and intelligent transport system at European level, by 2019. An objective that needs to face the technical and legal difficulties related to its effective implementation. The assessment of the impacts that the new system will produce on the right to privacy and data protection of modern drivers is one of the most complex issues.

Sommario: 1. La mobilità intelligente della C-ITS *Platform* – 2. Dati personali o non-personali? – 3. Le basi giuridiche per il trattamento di dati nel sistema C-ITS – 3.1. Perseguimento di un interesse pubblico (o adempimento di un obbligo legale) – 3.2. Consenso dell'interessato; 3.3. Esecuzione di un contratto – 3.4. Legittimo interesse del titolare –4. Molti i nodi ancora da

sciogliere – 4.1. Titolarità e allocazione delle responsabilità; 5. Uno sguardo al futuro della mobilità intelligente: non solo *privacy*.

1. La mobilità intelligente della C-ITS *Platform*

Sotto molti aspetti le automobili che guidiamo oggi possono già definirsi *connected device*, dispositivi che dialogano con il mondo esterno, ricevendo e trasmettendo informazioni. Sfruttando le potenzialità connettive di Internet, l'esperienza di guida dell'automobilista moderno viene arricchita e agevolata da avanzati sistemi di navigazione, servizi VoIP e di *infotainment*.

L'ultima frontiera dell'interazione macchina-ambiente è rappresentata dalla progettazione di veicoli intelligenti, capaci di comunicare tra loro senza necessità di intervento umano. Nel 2019 sarà inaugurato a livello europeo il primo sistema di trasporto intelligente (*Cooperative Intelligent Transport System*, C-ITS), in base al quale le autovetture in circolazione saranno in grado di comunicare tra loro e con altre infrastrutture di trasporto (come segnaletica stradale o apposite stazioni di recezione) scambiandosi informazioni utili alla circolazione.

Il progetto C-ITS nasce nel 2014 dall'esigenza di adottare una strategia europea comune per favorire la digitalizzazione nel settore dei trasporti e assicurare all'Europa una posizione competitiva nei confronti di paesi, come USA e Giappone, particolarmente all'avanguardia in questo campo.

L'obbiettivo del progetto nel breve periodo è accrescere la componente interattiva nella circolazione stradale per migliorare la sicurezza degli spostamenti e la gestione del traffico, guidando le scelte dell'automobilista. I veicoli sarebbero in grado di allertare i conducenti in merito a un incidente o un incrocio particolarmente trafficato prima di giungere sul luogo stesso, permettendo all'autista, per esempio, di modificare il proprio percorso scegliendo una strada alternativa. In una prospettiva di lungo termine, invece, il progetto mira a ridurre in maniera crescente l'intervento umano, automatizzando l'intera esperienza di guida attraverso l'introduzione di *autonomous vehicle* in grado di comunicare con i propri "simili" su strada e di prendere decisioni in maniera indipendente.

Per facilitare la celere ed efficiente attuazione del progetto, la Commissione europea ha creato la c.d. C-ITS *Platform,* una piattaforma di confronto e discussione, organizzata in commissioni specializzate nelle diverse aree di competenza (es. sicurezza; infrastrutture fisiche e digitali; *business model*), che nei passati tre anni ha iniziato ad analizzare le criticità del progetto dal punto di vista giuridico, tecnologico ed economico.
Tra le commissioni è stato creato in particolare un Gruppo di Lavoro dedicato alla valutazione dei profili concernenti la *privacy* e la protezione dei dati personali (*Data Protection and Privacy Working Group*). La portata del progetto e i meccanismi di comunicazione su cui esso è sviluppato porterebbero, infatti, alla più grande operazione di trattamento di dati mai effettuata. Lo scambio di informazioni tra veicoli e infrastrutture stradali coinvolgerebbe migliaia di enti e organizzazioni preposti al funzionamento del sistema (autorità pubbliche, industria automobilistica, società di telecomunicazioni ecc.) e milioni di automobilisti in tutta Europa. Le preoccupazioni sollevate dagli impatti che un tale colossale esperimento potrebbe avere sui diritti fondamentali dei cittadini europei non sono quindi infondate, soprattutto se considerate alla luce della nuova normativa europea *privacy* (regolamento (UE) 2016/679, GDPR), direttamente applicabile negli Stati Membri a partire da maggio 2018. Le rilevazioni fino ad ora prodotte dal Gruppo di Lavoro della Commissione[1] sono state recentemente sottoposte al vaglio dell'*Art. 29 Working Party* (WP29, Gruppo dei garanti *privacy* europei), che, pur circoscrivendo la materia delle proprie osservazioni, ha reso note per la prima volta le proprie osservazioni sul tema[2].

2. Dati personali o dati non-personali?

Premessa d'obbligo per valutare i possibili impatti sul diritto alla protezione dei dati personali dei cittadini europei è comprendere se il sistema C-ITS comporti effettivamente un trattamento di "dati personali" o se le informa-

[1] *Processing personal data in the context of C-ITS*, Document prepared by the Data Protection and Privacy Working Group of the C-ITS Platform for Art. 29, 10 July 2017 e *C-ITS Platform, Final report Phase II*, September 2017, entrambi consultabili al sito https://ec.europa.eu/transport/themes/its/c-its_en.

[2] *Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems* (C-ITS), adottata il 4 ottobre 2017.

zioni scambiate non possano invece considerarsi come dati-macchina, non riferibili a una persona fisica.

Per cercare di dare una risposta a questo preliminare quesito è necessario introdurre, pur con qualche semplificazione, il funzionamento del sistema C-ITS.

Come accennato, il sistema si fonda sullo scambio di messaggi tra veicoli (c.d. comunicazione V2V) e tra veicoli e infrastrutture stradali (c.d. comunicazione V2I o, piú in generale, V2X), all'interno di un'architettura a chiave pubblica (*Public Key Infrastructure,* PKI). La creazione di un sistema di comunicazione affidabile presuppone che i messaggi trasmessi e ricevuti siano autentici, provengano da fonti autorizzate e non possano essere modificati o falsati durante il transito. I processi e le tecnologie di crittografia a chiave pubblica garantiscono questo risultato. Attraverso l'attività congiunta di un ente di "iscrizione" (*enrollment authority*) e un'autorità di autorizzazione (*authorisation authority*), ogni veicolo parte del sistema C-ITS viene identificato (iscritto) e autorizzato, attraverso l'attribuzione di un certo numero di certificati digitali con i quali sarà in grado di "firmare" i messaggi inviati verso gli altri operatori della strada. I messaggi così "firmati" sono crittografati, pseudonimizzando la vera identità del mittente ma garantendo al tempo stesso l'autenticità della fonte e del contenuto. I soggetti riceventi, quindi, possono verificare la provenienza e l'integrità del messaggio grazie al certificato che vi è allegato, univocamente associato a uno specifico veicolo autorizzato.

I messaggi scambiati nel C-ITS sono di due tipologie, denominate CAM e DENM. Pur essendo entrambe finalizzate a fornire indicazioni sulle condizioni della circolazione stradale, si differenziano sia per il tipo di informazioni trasmesse, sia per le circostanze in presenza delle quali il messaggio è generato e inviato. I messaggi CAM (*Cooperative Awareness Message*), oltre al certificato che ne autentica contenuto e provenienza, contengono una serie di parametri identificativi del veicolo mittente come la sua velocità e localizzazione, le sue dimensioni e il suo peso. Tali messaggi vengono generati dagli autoveicoli in maniera automatica e continuativa, a scadenze temporali e spaziali predefinite, consentendo agli altri attori del circuito stradale di essere costantemente al corrente delle condizioni di guida e posizione del

veicolo mittente. A differenza dei CAM, che rappresentano lo strumento di comunicazione ordinario nel sistema C-ITS, i DENM (*Decentralised Environmental Notification Message*) costituiscono messaggi *una tantum*, generati in circostanze d'emergenza in cui il ritmo scadenzato dei messaggi CAM non riuscirebbe a raggiungere in tempo i destinatari per comunicare loro l'*alert.* È il caso, per esempio, di un incidente stradale o dell'improvviso peggioramento delle condizioni metereologiche su un tratto di transito. La necessità di informare tempestivamente della verificazione dell'evento attiva il meccanismo DENM, in base al quale i veicoli o le infrastrutture nei pressi dell'evento generano un messaggio immediato, contenente le informazioni rilevanti sull'accadimento, che viene istantaneamente trasmesso agli operatori stradali circostanti e si diffonde "rimbalzando" dall'uno, all'altro in una sorta di propagazione a macchia d'olio.

Alla luce di quanto illustrato il Gruppo di Lavoro e il WP29 si chiedono: i dati contenuti in CAM e DENM, quindi trasmessi all'interno del sistema, sono dati personali?

Il primo elemento da evidenziare è che entrambi i messaggi, in particolare i CAM, contengono informazioni inerenti al veicolo e non alla persona fisica che lo guida. Tale fatto non è però sufficiente a qualificare le informazioni trasmesse come "non personali", cioè riferibili esclusivamente alla macchina. È pacifico che indicazioni quali la posizione e le dimensioni del veicolo, soprattutto in contesti stradali scarsamente trafficati, siano da sole sufficienti ad individuare un singolo veicolo e quindi, indirettamente, il suo guidatore.

A ciò deve aggiungersi che sia i CAM sia i DENM contengono il certificato di autorizzazione generato dall'infrastruttura PKI. Dal certificato, associato come si è detto ad un veicolo mittente identificato e autorizzato, sarebbe quindi possibile risalire al proprietario fisico dello stesso. Benché il Gruppo di Lavoro puntualizzi che, al fine di associare l'intestatario del certificato ai dati di un determinato veicolo siano necessarie informazioni aggiuntive, detenute unicamente dal soggetto accreditatore, ciò non elimina di per sé il carattere personale dei dati trasmessi. Questi, tutt'al più, possono considerarsi dati "pseudonimizzati", sottoposti ad un processo che impedisce loro di essere collegati ad un interessato specifico senza l'utilizzo di informazioni aggiuntive, separatamente conservate (art. 4, n. 5 del GDPR). La pseudonimiz-

zazione, lungi dall'essere un meccanismo di anonimizzazione, è considerata sia dal GDPR sia dal WP29 come una misura di sicurezza aggiuntiva, che aiuta responsabili e titolari del trattamento a rispettare gli obblighi di protezione imposti dalla normativa.
Dunque, sia il Gruppo di Lavoro, sia il WP29 sono concordi nell'affermare che il C-ITS presuppone il trattamento dei dati personali degli automobilisti. Tale rilevazione ha un notevole impatto sull'attuazione del sistema. Nel caso di specie, infatti, trova piena applicazione la normativa europea in materia di protezione dei dati personali, cioè a breve il GDPR, che impone non solo il rispetto di generali e fondamentali principi di trattamento (quali necessità, trasparenza, minimizzazione e conservazione), ma anche la ricerca di un'adeguata base giuridica affinché il trattamento dei dati possa ritenersi legittimamente effettuato.

3. Le basi giuridiche per il trattamento di dati nel sistema C-ITS

Questo il quesito su cui si sono concentrati i maggiori sforzi del Gruppo di Lavoro e le maggiori preoccupazioni del WP29.
In base ai principi generali di trattamento dei dati personali, coloro che raccolgono, elaborano e comunicano dati personali possono farlo solo in presenza e nel rispetto di una delle condizioni ora elencate all'art. 6 del GDPR, tra cui si può annoverare: il consenso dell'interessato; l'esecuzione di un contratto; l'adempimento di un obbligo legale; il perseguimento di un interesse pubblico; il legittimo interesse del titolare e così via. Determinare quale dei presupposti elencati sia il più appropriato è essenziale per conferire legittimità al trattamento, evitando di incorrere nelle pesanti sanzioni previste dal regolamento *privacy*. In un contesto digitalizzato e dinamico, popolato da un'eterogenea platea di attori come il C-ITS, la valutazione si dimostra estremamente delicata e quanto mai complessa.

3.1. Perseguimento di un interesse pubblico (o adempimento di un obbligo legale)

Considerato che il primo e prevalente obbiettivo del progetto C-ITS è il miglioramento della sicurezza stradale e dell'efficiente circolazione, il presupposto giuridico che è parso più appropriato per effettuare il trattamento di

dati richiesto è il perseguimento di un interesse pubblico (art. 6, par. 1, lett. e) del GDPR). In base al disposto del regolamento *privacy*, l'interesse pubblico deve però essere previsto da una legge, nazionale o europea, che ne definisca chiaramente l'ambito di applicazione, possibilmente specificando i trattamenti autorizzati e necessari alla sua realizzazione. Il WP29 osserva inoltre che, alla luce delle finalità ultime perseguite dal progetto, cioè la diffusione di *smart car* automatizzate, è presumibile in un prossimo futuro che gli Stati decidano di introdurre in capo ai produttori un vero e proprio obbligo legale, che preveda l'inserimento di tecnologie C-ITS nei veicoli. In questo modo, la legittimità del trattamento sarebbe giustificata dalla necessità per gli operatori del sistema di ottemperare ad un obbligo di legge, come previsto dall'art. 6, par. 1, lett. c) del GDPR.
Il punto debole dei presupposti qui considerati è il tempo. Le stringenti scadenze per il debutto nel 2019 del sistema C-ITS non si conciliano con le lunghe tempistiche necessarie all'adozione di strumenti legislativi. Quindi, benché il WP29 incoraggi la Commissione europea ad iniziare al più presto i lavori per l'approvazione di un adeguato strumento normativo, al momento interesse pubblico o obbligo legale non sono opzioni praticabili per legittimare il trattamento di dati nel sistema C-ITS.

3.2. Consenso dell'interessato

In merito alla possibilità di legittimare il trattamento dei dati per mezzo della raccolta del consenso espresso dell'interessato-autista del veicolo (art. 6, par. 1, lett. a) del GDPR), il Gruppo di Lavoro, inizialmente fiducioso sulla sua concreta fattibilità, riscontra nel prosieguo dei lavori una serie di ostacoli alla sua realizzazione, poi confermati dallo stesso WP29. Il consenso, per essere valido, deve essere prestato liberamente, nei confronti di titolari identificati, per finalità specificatamente individuate e può in ogni caso essere sempre revocato dall'interessato (art. 7 e considerando 32 del GDPR). Tali requisiti non sono facilmente riscontrabili nel trattamento presupposto dal sistema C-ITS.
In primo luogo, la trasmissione delle comunicazioni nel sistema C-ITS avviene secondo un modello *peer-to-peer*, cioè ogni veicolo del sistema è al tempo stesso *client* e *server* delle informazioni trasmesse, e segue la mede-

sima logica della radio o telediffusione: le informazioni inviate dal veicolo mittente sono trasmesse nell'ambiente circostante senza sapere se o chi riceverà il messaggio. Ne consegue che gli attori del sistema non siano tra loro in un rapporto di comunicazione biunivoca e quindi che l'interessato automobilista non sia in grado di conoscere l'identità di tutti coloro che ricevono e utilizzano i suoi dati. Peraltro, il fatto che le modalità di trasmissione utilizzate dal sistema impediscano la creazione di una relazione tra soggetto mittente (interessato) e ricevente (titolare) rende estremamente difficile l'esercizio dei diritti posti in capo all'interessato, tra cui appunto quello di revocare il consenso in qualsiasi momento.
In secondo luogo, a causa della moltitudine di soggetti facenti parte del C-ITS, è difficile ipotizzare che possa essere richiesto un consenso specifico e distinto (come richiede il GDPR) per ciascuna delle diverse finalità perseguite dai soggetti che intendono trattare i dati.
Per tutte queste ragioni, sebbene il WP29 non neghi in assoluto il consenso quale adeguata base giuridica, la sua utilizzabilità nel caso di specie pare di difficile realizzazione.

3.3. Esecuzione di un contratto

La complessità relazionale che caratterizza il contesto C-ITS manifesta i suoi riflessi problematici anche nell'ipotesi in cui il trattamento di dati sia legittimato per mezzo dell'esecuzione di un contratto.
Il Gruppo di Lavoro tenta di colmare la mancanza di contatto diretto tra interessato e titolare, che come visto ostacola fortemente la prestazione di un valido consenso, proponendo un modello in cui tale rapporto possa costituirsi, a monte, attraverso il mezzo contrattuale. L'idea è quella di rendere il trattamento dei dati parte essenziale di un contratto sottoscritto, per esempio, tra colui che acquista un veicolo e i diversi operatori del sistema C-ITS, potenzialmente raggruppati in forma di consorzio.
Anche in questo caso, tuttavia, i rilievi del WP29 sono molteplici e riprendono in parte le argomentazioni critiche già espresse in tema di consenso. Innanzitutto, la condizione espressa dall'art. 6, par. 1 lett. b) del GDPR deve essere interpretata restrittivamente in quanto la necessità del trattamento di dati rispetto all'esecuzione del contratto deve essere ragionevolmente giusti-

ficata. Il trattamento effettuato con tale base giuridica presuppone, infatti, una preliminare analisi del contesto di trattamento che: individui i soggetti del trattamento; evidenzi le finalità per cui i dati dovrebbero essere utilizzati; chiarisca la compatibilità di tali finalità con un'esecuzione contrattuale e soprattutto delimiti le tipologie di dati che si ritengono "essenziali" ai fini dell'attuazione del contratto stesso. Tutti elementi il cui vaglio risulta in gran parte carente nei lavori eseguiti fino ad oggi dal Gruppo di Lavoro.

3.4. Legittimo interesse dei titolari

Infine, dopo aver scartato la possibilità di legittimare il trattamento per il perseguimento di un interesse vitale dell'interessato o di un terzo poiché non strettamente compatibile con le finalità perseguite dal C-ITS, il Gruppo di Lavoro ha considerato in ultima istanza la possibilità di avvallare il trattamento sulla base del perseguimento di un legittimo interesse del titolare del trattamento. Tra tutti i presupposti citati, questo è probabilmente quello di più ardua definizione in quanto, rifacendosi alla generica espressione "legittimo interesse" di una parte, richiede all'interprete una delicata opera di inquadramento. La *ratio* del presupposto si può ricondurre ad un generale principio di bilanciamento che impone di valutare gli interessi in gioco, soppesandone la reciproca prevalenza. In questo caso, il titolare (o meglio i titolari in considerazione del contesto C-ITS) dovrebbe dimostrare che il suo interesse, per quanto legittimo, non prevalga irragionevolmente sugli interessi e le libertà fondamentali degli interessati.

Si ripropongono quindi le medesime osservazioni avanzate in merito ai presupposti già esaminati. In questo caso, inoltre, il WP29 è ancora più incisivo nel ricordare che la delicatezza del settore di applicazione impone grande attenzione nell'identificazione della lunga catena di responsabilità coinvolte nel C-ITS, degli interessi legittimi perseguiti e dell'impatto di questi sui diritti e le libertà degli interessati, nonché la valutazione di adottare eventuali garanzie aggiuntive al trattamento per limitare le potenziali ripercussioni sugli interessati.

Ciò che il lavoro del Gruppo e le osservazioni del WP29 sembrano concludere è che nessuna delle basi giuridiche proposte risulta, al momento e da sola con-

siderata, base idonea a sostenere la legittimità di un trattamento di dati tanto consistente quanto rischioso come quello previsto nel sistema C-ITS.

4. Molti i nodi ancora da sciogliere

Il quadro risultante dalla sintetica analisi sopra esposta dimostra la grande difficoltà di inquadrare chiaramente le potenziali criticità e di trovare dunque possibili soluzioni al trattamento dei dati personali presupposto in un sistema articolato e tecnologico come il C-ITS. Sebbene sia da apprezzare l'indagine condotta fino ad oggi dal Gruppo di Lavoro, che ha iniziato a far luce su alcuni degli aspetti più critici del sistema, la percezione generale è che manchi una chiara messa a fuoco delle questioni da esaminare e dell'ordine logico con cui sarebbe necessario procedere per la loro analisi. La preliminare risoluzione di alcuni interrogativi, infatti, è condizione indispensabile per dare risposta ad altri. Come è stato rilevato anche dal WP29, per esempio, la chiara individuazione del modello di titolarità presupposto dal C-ITS è passaggio preliminare per la scelta della base giuridica più adatta per il trattamento.

4.1. Titolarità e allocazione delle responsabilità

Il tema della titolarità è stato parzialmente affrontato dal Gruppo di Lavoro, senza tuttavia il dovuto approfondimento, a cui è auspicabile sia riservata l'attuale "terza fase" dei lavori del Gruppo. La proposta emersa nel corso delle prime due fasi di analisi suggeriva di utilizzare il modello di contitolarità previsto dall'art. 26 del GDPR. Secondo il Gruppo di Lavoro, la lunga catena di titolari del trattamento coinvolti nel C-ITS potrebbe inquadrarsi sotto il profilo *privacy* in uno schema di contitolarità in cui tutti gli attori siano coinvolti nella direzione, gestione e vigilanza dei trattamenti richiesti dal sistema. Il WP29, a sua volta, precisa che l'adozione di una soluzione di contitolarità non deve essere concepita come una scorciatoia per sfuggire agli obblighi che il GDPR impone ai titolari e richiede perciò un'attenta ponderazione in merito al potere e alle responsabilità posti in capo ai diversi soggetti.

Anche in questo caso è possibile fin d'ora rilevare alcune criticità di fondo.

In primo luogo, il modello di titolarità sotto il profilo della *data privacy* dovrà necessariamente conciliarsi con il più generale modello di *governance* scelto per il sistema nel suo complesso. La definizione dello schema relazio-

nale tra gli attori del C-ITS si rifletterà inevitabilmente sulle scelte in materia di gestione e governo nel trattamento dei dati. Sembra quindi prioritario definire il modello di *governance* da adottare per l'attuazione del sistema e le modalità di interazione tra i diversi soggetti pubblici e privati coinvolti nel suo funzionamento.

In secondo luogo, la proposta di utilizzare il modello di contitolarità sembra stridere con la pluralità di funzioni e finalità che i titolari nel C-ITS intendono perseguire autonomamente. Come recita il GDPR, si ha una situazione di contitolarità del trattamento "allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento". Inoltre, "l'interessato può esercitare i propri diritti ai sensi del presente regolamento nei confronti di e contro ciascun titolare del trattamento". In base al dettato del regolamento *privacy*, la figura dei contitolari sembra identificare i casi in cui due o più soggetti condividono la decisione circa le finalità e i mezzi del trattamento dei dati. L'elemento della codecisione e quindi condivisione delle finalità perseguite sembra fattore centrale per distinguere una situazione di contitolarità da una situazione di titolarità autonome. Tale impianto appare difficilmente configurabile nel contesto C-ITS in cui i diversi soggetti del sistema (autorità pubbliche, produttori di veicoli, programmatori di *software*, società di telecomunicazioni ecc.), pur condividendone gli obbiettivi ultimi, tratterebbero ciascuno i dati per una finalità diversa, loro propria.

Alle difficoltà di individuare titolarità e base giuridica più appropriata, si affiancano poi numerose ulteriori interrogativi.

Ci si chiede quale sarà l'impatto del nuovo regolamento *e-privacy*[3] (ora in fase di adozione) sulle comunicazione trasmesse tra veicoli e infrastrutture. Le disposizioni del regolamento, a differenza di quanto attualmente previsto dalla direttiva 2002/58/CE, potrebbero applicarsi anche alle comunicazioni macchina-macchina, restringendo ulteriormente le condizioni di legittimità per il trattamento dei dati a favore di una più intesa protezione della riservatezza degli individui. Ancora molto, poi, è necessario valutare in merito

[3] Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (regolamento sulla vita privata e le comunicazioni elettroniche). COM/2017/010 final - 2017/03 (COD).

all'applicazione dei principi di *privacy by design* e *privacy by default* disciplinati dal GDPR, che sono strettamente connessi alle concrete modalità tecnologiche con cui il C-ITS sarà implementato; ugualmente si può dire per le misure di sicurezza che dovranno essere adottate dai titolari del trattamento al fine di minimizzare i rischi connessi all'identificazione dell'utente e all'utilizzo abusivo dei dati raccolti.

Quanto si è fin qui illustrato, seppur in maniera sintetica, rende evidenti le grandi potenzialità e le attuali profonde lacune del sistema di mobilità intelligente presentato dalla Commissione europea.

Il C-ITS è certamente da annoverare tra le innovazioni più attese dei prossimi anni, non solo per le modalità tecnologiche di attuazione ma anche per l'impatto rivoluzionario che avrà su innumerevoli importanti settori. I nuovi sistemi di interazione macchina-macchina e macchina-ambiente integreranno e progressivamente sostituiranno le imprecise e talvolta ingannevoli percezioni umane, con l'accuratezza oggettiva di sensori e programmi informatici, portando indubbi benefici collettivi: meno incidenti, più sicurezza stradale, migliore gestione del traffico e riduzione dell'inquinamento.

Date le dimensioni del progetto e le potenziali implicazioni sulla *privacy* di milioni di cittadini, stupisce che, ad oggi, poco ancora si sia chiarito in merito e che moltissime rimangano le questioni aperte. Gli sforzi del Gruppo di Lavoro non sono fino ad oggi stati sufficienti per dare un solido inquadramento al trattamento di dati personali previsto nel sistema C-ITS. Le osservazioni del WP29, che conservando il ruolo di autorità indipendente mantiene una certa distanza dai lavori della Commissione europea, sembrano sollevare nuove incertezze. Allo stesso tempo, alcuni Garanti nazionali (tra cui il CNIL, Garante *privacy* francese) si sono mossi autonomamente, adottando linee guida nazionali[4] che forniscono un'interpretazione del sistema in base alla normativa *privacy* nazionale e al GDPR.

Se la data di scadenza per l'inaugurazione del progetto è fissata per il 2019, il 2018 si prefigura come l'anno in cui la C-ITS *Platform* dovrà tirare le somme e presentare i risultati del suo lavoro, nella speranza che, soprattutto

[4] *Commission Nationale Informatique & Libertès* (CNIL), *Compliance package – connected vehicles and personal data*, adottato nell'ottobre 2017.

in materia di *privacy* e protezione dei dati personali, il prodotto di quattro anni di lavoro sia sufficientemente convincente da ottenere l'approvazione delle autorità garanti europee.

5. Uno sguardo al futuro della mobilità intelligente: non solo *privacy*

A conclusione del presente contributo, sembra utile offrire al lettore una panoramica più ampia e, per così dire, lungimirante sul settore della mobilità intelligente, al di là di profili strettamente connessi a *privacy* e protezione dei dati personali.

Abbiamo fin qui parlato di un sistema, il C-ITS, finalizzato ad introdurre sul circuito stradale veicoli in grado di aiutare i propri guidatori alla migliore gestione della circolazione stradale. Sebbene il veicolo acquisti una parziale autonomia in termini di comunicazione e interazione con i diversi attori della strada, in questa prima fase di implementazione l'individuo continua ad esercitare un ruolo attivo di controllo sullo stesso.

Si è accennato, tuttavia, che nel lungo termine il sistema mira a sposare il progetto di "mobilità connessa" con quello di "mobilità autonoma", portando alla creazione di macchine in grado non solo di comunicare tra loro e con l'ambiente circostante ma anche di prendere decisioni in maniera autonoma, in base alle informazioni ricevute. Un nuovo modello, quindi, che cambierebbe in maniera radicale il paradigma di mobilità: da guidatore-agente e veicolo-strumento a guidatore-soggetto (semi) passivo e veicolo-agente autonomo.

Queste considerazioni aprono le porte all'articolato dibattito, che ha avuto inizio negli ultimi anni, sulle conseguenze giuridiche, sociali ed economiche legate agli sviluppi della robotica e dell'intelligenza artificiale, nel cui ambito si colloca lo specifico settore della mobilità autonoma. Tra i documenti che offrono in rassegna il diversificato ventaglio di problematiche sollevate dall'evoluzione tecnologica, rimane ad oggi significativa la risoluzione del Parlamento europeo recante raccomandazioni concernenti norme di diritto civile sulla robotica[5], adottata il 16 febbraio 2017. Nelle sue parole introdut-

[5] Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL)).

tive, la risoluzione prende atto degli inarrestabili cambiamenti tecnologici a cui sta andando incontro la società odierna, che "sembrano sul punto di avviare una nuova rivoluzione industriale, suscettibile di toccare tutti gli strati sociali" e invita all'apertura di un dialogo, a livello nazionale e soprattutto europeo, per discuterne le implicazioni e le conseguenze sul piano legale ed etico. È evidente che molti sono i temi che necessitano di approfondimento: da considerazioni in merito al finanziamento e supporto della ricerca e innovazione, a valutazioni circa l'adozione di principi etici di orientamento nello sviluppo della robotica; dall'analisi degli impatti giuridici in settori quali proprietà intellettuale e (come si è visto) protezione dei dati personali, alla definizione di norme tecniche in materia di sicurezza, protezione e interoperabilità.

Tuttavia, tra le questioni accennate dalla risoluzione, una ha sollevato particolare interesse nel mondo giuridico: la responsabilità civile per danni causati da *robot.*

Come già illustrato, i progressi tecnologici hanno reso o renderanno nel prossimo futuro i *robot* sempre più complessi e sempre più simili ad agenti autonomi. Ciò rende l'allocazione di responsabilità per le azioni delle macchine una questione spinosa, sia in considerazione dell'elevato numero di attori che rivestono un ruolo attivo nella produzione e nell'utilizzo della macchina stessa (si pensi a produttori, programmatori, operatori di manutenzione, proprietari e utilizzatori), sia considerando che all'aumentare dell'autonomia decisionale delle macchine, diminuisce il potere di controllo umano sulle loro azioni.

Si pone quindi il problema di valutare se l'attuale quadro giuridico in materia di responsabilità sia sufficiente ad individuare la responsabilità legale dei soggetti per le azioni e omissioni imputabili ai *robot*, qualora le cause non possano essere ricondotte ad un soggetto specifico.

Nel tentativo di organizzare una prima linea riflessione, la risoluzione propone diverse soluzioni giuridiche.

Una prima proposta concerne l'introduzione di un sistema basato sulla responsabilità oggettiva (da stabilire se in capo al produttore, al proprietario o all'utilizzatore), che agevoli la prova del danno e quindi le possibilità di risarcimento. In alternativa, viene suggerita la previsione di una responsabilità basata su un approccio di c.d. "gestione dei rischi", secondo il quale deve re-

sponsabilizzarsi il soggetto in grado di minimizzare i rischi e di affrontare gli impatti negativi (probabilmente, quindi, il produttore). Il pericolo, in questi casi, sarebbe quello di penalizzare solamente alcune categorie di individui, facendo loro sopportare i costi sociali dell'automazione. Nel settore automobilistico, per esempio, tale modello potrebbe tradursi in un aggravio della responsabilità in capo al conducente (e, in subordine, al proprietario) del mezzo, o alla riformulazione, in termini meno stringenti, dell'attuale "responsabilità da prodotto" del produttore[6]. Nessuna delle due sembra però rappresentare una soluzione assolutamente convincente. Nella prima ipotesi, infatti, l'imputazione del danno anche in assenza di colpevolezza avrebbe ricadute eccessivamente gravose, dal punto di vista giuridico ed economico, sui singoli individui; nella seconda ipotesi, benché da preferirsi alla prima, il rischio sarebbe quello di disincentivare gli investimenti nella ricerca e sviluppo del settore.

Per agevolare la ripartizione di responsabilità, è interessante la proposta di istituire un regime assicurativo obbligatorio (sulla linea della r.c. auto) imposto a produttori e proprietari di *robot* autonomi, eventualmente affiancato dalla creazione di un fondo di risarcimento per garantire il ristoro dei danni, anche in assenza di copertura assicurativa. In alternativa ad un regime assicurativo obbligatorio, la risoluzione propone un regime di responsabilità limitata per quei produttori, programmatori, proprietari o utilizzatori che si assicurino congiuntamente contro i possibili danni causati da *robot* autonomi e, a tale scopo, costituiscano un fondo di risarcimento. Nel settore automobilistico, dove per l'appunto è già presente un sistema di assicurazione obbligatoria sui veicoli, il modello potrebbe tradursi in una rimodulazione dell'attuale r.c. auto in base alle nuove esigenze di tutela connesse all'utilizzo di *autonomous car*, includendo tra i soggetti destinatari obbligati

[6] Per approfondire il tema della responsabilità nel futuro automobilistico delle *driverless car* si rinvia all'interessante articolo di A. Davola – R. Pardolesi, *In viaggio col robot: verso nuovi orizzonti della r.c. auto ("driverless")?*, in *Danno e resp*., 5/2017, 616-629. Si veda inoltre M.C. Gaeta, *Automazione e responsabilità civile automobilistica,* in *Resp.civ.prev.,* 5/2016, 1718-1750.

Più in generale, per una rassegna delle soluzioni proposte per colmare il *responsibility gap* creato dall'automazione robotica, si rinvia al contributo di E. Palmerini, *Robotica e diritto: suggestioni, intersezioni, sviluppi a margine di una ricerca europea*, in *Responsabilità civile e previdenza,* 6/2016, 1816-1850.

non solo i proprietari dei veicolo ma anche i produttori o programmatori degli stessi[7]. Tuttavia, la criticità dei modelli che introducono una componente assicurativa risiede nelle difficoltà connesse alla valutazione del rischio e del potenziale danno, necessarie per quantificare il premio assicurativo. Tali valutazioni, basandosi sul calcolo probabilistico circa la verificazione di determinati eventi e l'ammontare delle possibili ripercussioni, sono estremamente difficili da effettuare in settori agli esordi, privi di una base statistica rilevante e attendibile.

Infine, alquanto singolare è stata la proposta del Parlamento europeo di valutare l'istituzione di uno *status* giuridico specifico per i *robot*. Sarebbe una sorta di "personalità elettronica" che permetta di considerare i *robot* come autonomi centri di imputazione e, dunque, di responsabilità nel risarcimento dei danni da loro causati. L'intento della proposta non è evidentemente quello di elevare le persone elettroniche a centri di diritti e doveri alla pari delle persone fisiche, quanto più quello di costituire un centro unico di imputazione della responsabilità. Tale proposta, quindi, dovrebbe leggersi in combinato disposto con la creazione di un registro di identificazione dei *robot* in commercio e con un fondo di risarcimento, finanziato dai soggetti partecipanti alla catena di produzione e utilizzazione del *robot*, dal quale attingere per la riparazione dei danni[8]. Non sono mancati, anche in questo caso, i rilievi critici che evidenziano il rischio di generare equivoci nell'attribuzione di soggettività giuridica ad un ente-macchina, aprendo la strada a quelle correnti di pensiero che sostengono l'equivalenza tra persona umana e intelligenza artificiale, anche sul piano giuridico.

In definitiva, molti gli spunti di riflessione, poca ancora la chiarezza sul da farsi.

La rapida e incessante trasformazione tecnologica a cui sta andando incontro la nostra società porterà con sé inevitabili conseguenze sul piano giuridico.

---

[7] Cfr. A. Davola – R. Pardolesi, *In viaggio col robot: verso nuovi orizzonti della r.c. auto ("driverless")?*, cit., 628 che introducono il tema di una possibile rimodulazione della r.c. auto nel senso tuttavia di responsabilizzare principalmente il produttore, creando una forma di polizza simile alle attuali "r.c. prodotti".

[8] Cfr. sul punto E. Palmerini, *Robotica e diritto: suggestioni, intersezioni, sviluppi a margine di una ricerca europea*, cit., 1835.

Le macchine diventeranno nel tempo sempre più complesse, sempre più interattive, sempre più autonome, ponendosi come protagoniste nello svolgimento di un numero crescente di attività umane. Le questioni giuridiche sollevate da tale cambiamento sono diverse, prime fra tutte un'analisi degli impatti sulla *privacy* e protezione dei dati personali degli individui e una rivalutazione del tradizionale regime di responsabilità civile.

Nell'eterna rincorsa tra diritto e tecnologia, sembra arrivato il momento di impegnarsi nell'apertura di un serio dialogo, soprattutto a livello legislativo, per dare certezza giuridica alle problematiche sopra illustrate, onde evitare che l'imposizione di fatto dei nuovi modelli tecnologici trovi il diritto (ancora una volta) impreparato ad affrontarne i risvolti legali. Ciò appare tanto più urgente in un settore come quello della mobilità intelligente, la cui implementazione, lungi dall'essere un'utopia asimoviana, è ormai a un passo di distanza.

Diritto Mercato Tecnologia

Numeri Speciali

2016 Lo Statuto Etico Giuridico dei Campioni Biologici Umani
a cura di Dario Farace

La rivista "Diritto Mercato Tecnologia" intende fornire un costante supporto di aggiornamento agli studiosi e agli operatori professionali nel nuovo scenario socio-economico originato dall'interrelazione tra diritto, mercato e tecnologia, in prospettiva interdisciplinare e comparatistica. A tal fine approfondisce, attraverso studi nei settori privatistici e comparatistici, tematiche afferenti in particolare alla proprietà intellettuale, al diritto antitrust e della concorrenza, alle pratiche commerciali e alla tutela dei consumatori, al biodiritto e alle biotecnologie, al diritto delle comunicazioni elettroniche, ai diritti della persona e alle responsabilità in rete.