IAIC MiBACT DGBIC CREDA

DIRITTO MERCATO TECNOLOGIA

FONDATA E DIRETTA DA
Alberto M. Gambino

COMITATO DI DIREZIONE
Valeria Falce, Giusella Finocchiaro, Oreste Pollicino,
Giorgio Resta, Salvatore Sica

27 ottobre 2018

L'IoT nel settore automotive: problematiche privacy on board e on road

Alessio Cantone

Nuova Editrice Universitaria

La rivista è stata fondata nel 2009 da Alberto M. Gambino ed è oggi pubblicata dall'Accademia Italiana del Codice di Internet (IAIC) sotto gli auspici del Ministero dei beni e delle attività culturali e del turismo - Direzione generale biblioteche e istituti culturali (DGBIC) e dell'Università Europea di Roma con il Centro di Ricerca di Eccellenza del Diritto d'Autore (CREDA).

Norme di autodisciplina

1. La pubblicazione dei contributi sulla rivista "Diritto Mercato Tecnologia" è subordinata alla presentazione da parte di almeno un membro del Comitato di Direzione o del Comitato Scientifico e al giudizio positivo di almeno un membro del Comitato per la Valutazione Scientifica, scelto per rotazione all'interno del medesimo, tenuto conto dell'area tematica del contributo. I contributi in lingua diversa dall'italiano potranno essere affidati per il referaggio ai componenti del Comitato Scientifico Internazionale. In caso di pareri contrastanti il Comitato di Direzione assume la responsabilità circa la pubblicazione.
2. Il singolo contributo è inviato al valutatore senza notizia dell'identità dell'autore.
3. L'identità del valutatore è coperta da anonimato.
4. Nel caso che il valutatore esprima un giudizio positivo condizionato a revisione o modifica del contributo, il Comitato di Direzione autorizza la pubblicazione solo a seguito dell'adeguamento del saggio.

La Rivista adotta un Codice etico e di buone prassi della pubblicazione scientifica conforme agli standard elaborati dal Committee on Publication Ethics (COPE): Best Practice Guidelines for Journal Editors.

Sede della Redazione

Accademia Italiana del Codice di Internet, Via dei Tre Orologi 14/a, 00197 Roma, tel. 06.8088855, fax 06.8070483, www.iaic.it, info@iaic.it

L'IoT NEL SETTORE AUTOMOTIVE: PROBLEMATICHE PRIVACY ON BOARD E ON ROAD

Alessio Cantone

Sommario: 1. Premessa – 2. La sicurezza del veicolo e dei passeggeri – 3. La tenuta della privacy nei servizi di infotainment – 4. La tutela della privacy nei servizi delle *insutech* – 5. *Smart road* e privacy: ancora qualche criticità – 6. Conclusioni

Abstract: Prendendo a prestito una delle note definizioni di IoT, il cui nucleo principale è di garantire che le cose siano connesse in qualsiasi momento, ovunque, con qualsiasi cosa e da chiunque utilizzi idealmente qualsiasi rete e qualsiasi servizio, non vi è dubbio che il settore automotive sia pienamente investito da questa ennesima rivoluzione tecnologica, basti pensare che entro il 2020 questo mercato varrà 113 miliardi di euro. L'intento di questo breve articolo è di cercare di fare un po' di chiarezza sulle problematiche privacy legate al mondo delle cosiddette "*connected car*", alcune di esse meritevoli di particolare attenzione altre, potrebbero risultare fortemente ridimensionate.

By borrowing one of the most known definition of IoT, the core of wich is to enable things to be connected anytime, anyplace, with anything and anyone ideally using any path/network and any service, there is no doubt that car industry is fully involved by this umptheenth tecnological revolution, just think by 2020 this market will be worth 113 billions of euro. The aim of this article is to try to do some clarify about privacy issues related to the world of connected car, some of them deserving of special attention, the others could be significantly scaled.

1. Premessa

Durante la realizzazione di questo contributo ho notato che moltissimi articoli riguardanti l'applicazione al settore automotive delle tecnologie IoT, a mio modesto avviso, creerebbero molta confusione su quelle che sono le problematiche privacy rinvenibili in questo specifico settore. Un piccolo caos prodotto dalla tendenza di inserire in un unico calderone − quello generico della sicurezza − criticità che dovrebbero essere suddivise ed esaminate singolarmente, per poi capire se sussistono concrete violazioni della nostra privacy, quale sia il loro grado di gravità e come porvi rimedio. Ecco, dunque, che si procederà ad un'analisi di quelle che ritengo le principali problematiche emerse in tema di "auto connesse", come quelle riguardanti la sicurezza del veicolo e, dunque, anche dei conducenti e quelle inerenti la sicurezza dei dati personali, nel momento in cui essi si rivelano preziosi per attivare servizi commerciali (particolarmente nell'ambito *Insutech*) nonché funzionali a garantire il progressivo sviluppo del cd *Intelligent Transport System*.

2. La sicurezza del veicolo e dei passeggeri

Un futuro che sembrava lontano è piombato impetuosamente nel presente con una tale velocità che, lo stupore creato dalla possibilità di accedere ad una serie di servizi e di informazioni premendo un semplice tasto sul volante, ha fatto dimenticare ai più (su tutti l'industria automobilistica) una regola semplicissima: ogni device collegato alla rete è attaccabile. Il massiccio impiego delle tecnologie *on-board* rendono il veicolo un dispositivo esposto a rischi paragonabili a quelli dei tradizionali pc. Procedendo ad un'analisi prettamente giuridica di quelle che possono essere le conseguenze delle vulnerabilità delle connected car sulla privacy dei loro passeggeri, nella stragrande maggioranza dei contributi è sempre riportato il noto caso di carhacking a danno della Jeep Cherokee.[1]

[1] A. Greenberg, *Hackers remotely kill a jeep on the highway with me in it*, reperibile in https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/. Nel luglio di 2015, due ricercatori di sicurezza informatica, Charlie Miller e Chris Valasek hanno uti-

***

Il presente contributo è stato da ultimo rivisto a luglio 2019

***

Mi sono chiesto se, eventi quali modificare la velocità dell'auto, agire sul sistema frenante, manipolare il condizionatore ecc, potessero essere catalogati quali esempi di violazione della privacy dal momento che, a ben vedere, riguardano prettamente l'incolumità fisica dei conducenti. Si badi bene, non si vuole affermare che la cyber sicurezza dell'industria automobilistica non sia strettamente connessa con la tutela della privacy ma, sottolineerei la necessità di riportare esempi diversi (magari meno sensazionalistici) dai quali si possano evincere, in maniera più forte e diretta, le conseguenze che l'hacheraggio di un auto ha sulla nostra sfera privata. Ad esempio, proprio nel caso di scuola della Jeep di cui sopra, molti hanno sottolineato come il sistema multimediale e multidevice U-Connect, grazie al collegamento a Internet tramite la rete mobile Sprint, conferisce agli hacker − utilizzando un dispositivo mobile della stessa rete come hot spot Wi-Fi e un computer − di scovare eventuali vulnerabilità della rete. In pochi si sono soffermati sul fatto che, una volta trovato un bersaglio appropriato, gli attaccanti sono in grado di recuperare informazioni su quel veicolo, come il numero di identificazione dello stesso, la marca, il modello, l'indirizzo IP e, soprattutto, le coordinate GPS del veicolo bersaglio e, dunque, tracciarne la posizione. Era il 2015 e, sebbene gli obiettivi erano veicoli apparentemente casuali e gli hacker non erano all'epoca in grado di ottenere informazioni personali, i ricercatori Miller e Valasek dichiararono che non era impossibile hackerare un'auto

---

lizzato le ultime tecniche di hacking per attaccare i sistemi elettrici di una Jeep Cherokee, senza accedere fisicamente al veicolo. Attraverso Internet sono riusciti a ottenere il controllo wireless della Jeep Cherokee, che gli ha permesso di accedere al sistema di intrattenimento, alle funzioni del cruscotto e consentendogli di controllare freni, sterzo e trasmissione. Tutto questo a distanza di alcuni chilometri dalla posizione del veicolo. Per una dettagliata analisi delle problematiche in materia di carhacking cfr., C. Smith, *Il manuale dell'hacker di automobili: Guida per il penetration tester*, Milano, 2016.

appartenente a una persona specifica, tracciando gli spostamenti e analizzando le sue abitudini di viaggio[2].

Alcuni anni prima di questo noto carhacking, la divisione cyber security del Department of Homeland Security's Science and Technology Directorate (DHS S&T) degli Stati Uniti, cercava il modo di recuperare ed analizzare la mole di dati raccolti dai sistemi di infotainment (o meglio dai processori che gestiscono questi sistemi) che potevano risultare utilissimi in alcune indagini di polizia (tanto che l'articolo parla di "vehicle forensics")[3]. Per fare ciò, avviarono una collaborazione con la società Enter Berla, creando il Project iVe. Un tool costituito da un hardware per estrarre dati dai sistemi informatici presenti in auto e un software che consente di analizzarli. Non è un caso che parli al plurale di sistemi informatici dal momento che, secondo il Ceo di Berla, per ogni singola nuova auto prodotta negli Usa, ci sono circa 70 differenti computers e, in alcuni modelli, anche oltre 100 processori necessari per processare ogni ora una mole di dati pari a 25 gigabytes[4]. Ma lo stupore non finisce qui. La società nel 2013 affermava di essere riuscita ad hackerare circa 80 differenti modelli di auto, per passare ad oltre 4.600 auto nel 2017. Il Ceo della società spiegò che, una volta trovata una vulnerabilità nel sistema di un modello di auto, si riusciva facilmente ad accedere agli altri diversi sistemi presenti in altri modelli, in barba alla tanto sbandierata *privacy and security by design*[5]. In poche parole, una volta collegato lo smartphone via

---

[2]T. Foglia, *Carhacking: 5 terribili metodi per hackerare un'auto*, reperibile in www.alground.com/site/carhacking-hackerare-auto/49208/

[3] Sul delicato rapporto tra lo sviluppo della tecnologia per la prevenzione ed accertamento delle attività criminali e i diritti della persona Cfr, A. Pierucci, *La protezione dei dati tra esigenze di sicurezza e diritti delle persone*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), *Il codice di trattamento dei dati personali*, Torino, 2007, pg 1030

[4] In merito alle problematiche connesse ai big data, in particolar modo quelle inerenti la proprietà degli stessi Cfr V.Zeno-Zenchovic, *Dati, grandi dati, dati granulari e la nuova epistemologia del giurista*, in *Riv. Dir. Media*, 2/2018, pp 1-8

[5] L. Bolden, D. Myrie, *Car tech privacy: Your car's infotainment system might be grabbing data from your phone*, su https://www.clickorlando.com/news/investigators/car-tech-privacy-your-cars-infotainment-system-might-be-grabbing-data-from-your-phone;
Sui concetti di privacy by design e by default, L. Bianchi, G. D'Acquisto *(Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita art.25)* in G.M.Riccio, G.Scorza, E. Belisario (a cura di), *GDPR e normativa privacy. Commentario,* Milano, 2018, pp. 245-258. Per un'analisi tecnico-scientifica Cfr, G. D'acquisto,

Bluetooth o Usb al sistema di infotainment, quest'ultimo, non solo raccoglieva indiscriminatamente tutto quello che avevamo sul telefono (dalla rubrica, alle foto, ai video) ma, una volta archiviato il tutto su un cloud, quei dati erano scarsamente protetti.

Nel 2017 il CNR di Pisa ha dimostrato come le auto, che utilizzano un sistema di infotainment basato sul sistema operativo Android e connesse al sistema Can bus dell'auto, possono fornire dei punti d'accesso ad utenti o per processi non autorizzati. A tal proposito, l'installazione di applicazioni non provenienti da store ufficiali, potrebbero nascondere dei malware che permettono l'accesso da remoto al dispositivo infotainment. Sfruttando una simile vulnerabilità, è possibile costruire un'applicazione ad hoc che, una volta installata sul dispositivo, permetta all'attaccante di accedere a diverse informazioni sia del guidatore che del veicolo stesso. Una volta installata l'applicazione malevola è possibile, ad esempio, effettuare una registrazione ambientale dell'abitacolo e scattare foto dalle telecamere di parcheggio[6].

Sono ancora dei ricercatori italiani a soffermarsi sulle vulnerabilità di Android auto stabilendo, a seguito dei test effettuati, che quasi l'80% delle apps riguardanti sistemi di infotainment disponibili nel play store di Google sono vulnerabili. Sembra paradossale eppure, più vi è la tendenza a sviluppare sistemi altamente sofisticati ed evoluti per rispondere alle richieste del cliente, più è facile riscontrare delle minacce per la sicurezza delle nostre informazioni[7].

M.Naldi*, Big data e privacy by design. Anonimizzazione, Pseudonimizzazione, Sicurezza*, Torino,2017.

[6] CNR, *La tua auto ti spia*, reperibile in http://www.cnrweb.tv/la-tua-auto-ti-spia; altro tipo di attacco è il CAN Hacking Tool (CHT) che è in grado di consentire ad un hacker di prendere il controllo di un'auto sfruttando il sistema operativo installato a bordo. Bastano pochissimi minuti per montare a bordo questo dispositivo grosso come il palmo di una mano e il gioco è fatto. Con quattro fili collegati alla Controller Area Network, l'hacker è in grado di controllare in remoto fari, serrature, sterzo, freni e air bag. Il chip dunque riesce a bypassare il sistema di crittografia andando a scrivere direttamente all'interno della centralina dell'auto. Il prototipo realizzato da alcuni ricercatori spagnoli specializzati in sicurezza, Javier Vazquez Vidal e Alberto Garcia Illera.

[7] A. Mandal; A. Cortesi; P. Ferrara; F. Panarotto; F. Spoto, *Vulnerability Analysis of Android Auto Infotainment Apps*, 2018, reperibile in http://www.pietro.ferrara.name/2018_CF.pdf *All the infotainment apps available in Google Play Store have been checked against that list of possible exposure scenarios. Results show that almost 80% of the apps are vulnerable, out of*

Nell'attesa che i giganti del web e l'industria automobilistica depongano quanto prima l'ascia di guerra, smettendo di preoccuparsi di chi favorisce cosa nei loro sistemi di infotainment, avviando una seria e proficua collaborazione volta ad eliminare le vulnerabilità ancora oggi riscontrate, le prime indispensabili azioni da compiere sono a carico del consumatore. Aldilà di quelli che sono i necessari interventi dell'ingegneria per rendere by design un software auto sicuro[8], per grandi linee, le regole da seguire sembrerebbero le stesse valide per tutte le tipologie di phishing: massima vigilanza, una sana diffidenza ad aprire link sospetti o esca, aggiornare sempre il sistema operativo all'ultima versione disponibile ed essere pronti a recepire le patch del produttore. Insomma, come sempre, una buona fetta di sicurezza informatica passa da una elementare, quanto imprescindibile, consapevolezza dei rischi informatici.

3. La tenuta della privacy nei servizi di infotainment

Se nel paragrafo precedente sono state indicate alcune vulnerabilità informatiche rinvenute nei sistemi di infotainment che − di riflesso − mettono a serio rischio la nostra privacy, verrebbe da chiedersi se questa venga tutelata, nel momento in cui decidiamo di avvalerci di alcuni dei servizi offerti da tali sistemi multimediali. Il termine infotainment è un neologismo di derivazione anglosassone, che letteralmente unisce le parole information ed entertainment; in particolare, quello presente *in vehicle* (IVI; in alcuni casi anche noto come ICE, *In-car entertainment*), è una architettura complessa di componenti hardware e software, che fornisce intrattenimento audio/video. La stragrande maggioranza si presenta come uno schermo touchscreen inserito nella plancia della vettura, con una interfaccia utente intuitiva

---

which 25% poses security threats related to execution of JavaScript; […] Android Auto also allows one to interact with multiple devices connected to the car. This in turn leaves automobiles in a potentially vulnerable state in front of adversaries, as it provides many attack surfaces from multiple connections such as cellular, Wi-Fi, Bluetooth etc.

[8] G. Dini, *Software sicuro per auto connesse, le regole per renderlo "a prova di hacker"*, reperibile in https://www.agendadigitale.eu/sicurezza/auto-connesse-software-a-rischio-hacker-le-regole-per-renderlo-sicuro/

e semplice come quella in modalità touchpad ma, siccome la tecnologia avanza incalzante, al giorno d'oggi gran parte delle funzioni multimediali, quali l'avvio di gps, di telefonate, la gestione del climatizzatore e della radio ed altro ancora, vengono gestite attraverso comandi vocali o pulsanti touch control sul volante. Per scongiurare pericolose distrazioni durante la guida, nel giro di alcuni mesi si assisterà all'ennesima evoluzione consentendo all'utente di rivolgersi all'assistente vocale, fornendo indicazioni che gli permetteranno d'imparare abitudini e preferenze, raggiungendo un grado di conoscenza tale da anticipare i bisogni stessi dell'utente. Per esempio, potrebbe impostare le stazioni radio, scegliere destinazioni di navigazione in base al giorno e all'orario. Insomma, la quantità di informazioni che questi sistemi possono raccogliere sono tante e destinate sempre più ad aumentare.

All'esito di un difficoltoso reperimento di alcune policies sul funzionamento di questi sistemi, si può ritenere che − per grandi linee − tre grandi categorie di dati sono potenzialmente trattate: dati anagrafici, i dati di navigazione (compresi indirizzo IP, tempo di accesso sul sito web, informazioni sulle pagine visitate dall'utente all'interno del sito web, tempo di navigazione su ciascuna pagina, ecc) e i cookies. A queste categorie, corrispondono altrettante tre basi giuridiche che legittimano il trattamento dei dati forniti dagli acquirenti di autovetture: quella dell'esecuzione del contratto, del consenso dell'interessato (nell'ambito di attività di marketing e profilazione) e dell'interesse legittimo (riguardo ad indagini di mercato)[9]. Si consideri che, se da un punto di vista logico-giuridico l'individuazione delle condizioni di liceità ex art. 6 del GDPR sembrerebbe corretta, in realtà, nell'analizzare alcune informative e condizioni generali di utilizzo dei servizi di infotainment di alcuni noti gruppi automobilistici, tutto emerge tranne che *informazioni*

[9] Se, in base al *considerando* 47, il trattamento dei dati per finalità di marketing diretto può essere considerato legittimo interesse, a maggior ragione può fondarsi su tale base di legittimità l'attività di customer satisfactation. Non solo, perché palesemente meno tediosa della precedente ma, anche, perché l'interessato può ragionevolmente aspettarsi quel tipo di elaborazione dei dati ad opera del venditore.

concise, trasparenti, intelligibili e facilmente accessibili sul trattamento dei dati personali[10].

Se si considera che alcuni servizi (principalmente quelli di navigazione) sono erogati da partner della casa costruttrice, che avranno la facoltà di imporre i propri termini e condizioni, ed aggiungerei anche le rispettive policies sulla privacy, ecco il moltiplicarsi del numero di documenti che l'interessato/acquirente avrà la briga di leggere, in quanto esse non vengono nemmeno riportate sommariamente nei principali documenti da firmare. Ma questo è il minore dei mali. Proseguendo nell'analisi della documentazione inerente questi sistemi multimediali e multidevice si legge che, qualora l'acquirente decida di vendere il veicolo senza aver previamente informato la casa automobilistica quest'ultima, non solo nega la propria responsabilità in caso di ulteriore raccolta dei dati ritenendo, in buona fede, che gli stessi appartengano all'originario proprietario ma, è esonerata da qualsiasi responsabilità, anche in caso di danni derivanti da violazioni connesse al trattamento dei dati personali. Gruppi automobilistici di fama mondiale potrebbero e dovrebbero fare molto di più per tutelare i nostri dati, piuttosto che invocare la buona fede (ad esempio, si potrebbe iniziare ad ipotizzare l'invio di sms e/o far comparire sul display dello schermo, a cadenza periodica, un promemoria sulla necessità di avvertire il produttore di un eventuale passaggio di proprietà, onde provvedere alla totale cancellazione dei dati finora raccolti). Per non parlare dell'altra clausola di manleva nel caso in cui, agendo da remoto per il controllo e aggiornamento della componente hardware e software, dovesse esserci una involontaria perdita di dati. A suffragare l'idea che ci si trovi di fronte ad una situazione allarmante per la protezione dei nostri dati, in un documento della Federal Trade Commission e della National Highway Traffic Safety Administration, si ribadisce più volte l'importanza di dover cancellare tutti i dati riguardanti proprietari, conducenti e passeggeri, riportando il veicolo allo stato di fabbrica. Dal momento che i veicoli motorizzati raccolgono sempre più dati personali e sono così facilmente utilizzabili da terze parti (attraverso noleggio o passaggi di proprietà), è opportuno prestare la

[10] Così come affermato dal Gruppo di lavoro ex art. 29, nelle linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679, ult.vers. del 06/02/2018- WP251 rev.01.

massima attenzione nel procedere alla cancellazione dei dati e a testare, non solo la sicurezza delle reti ma, anche, delle piattaforme sulle quali vengono archiviati[11].

Non vi è ombra di dubbio che imbattersi in clausole che cercano di tutelare l'azienda a 360 gradi, anche nelle più remote possibilità di una sua responsabilità legale, sia naturale e faccia parte del gioco delle parti. Tuttavia fa un certo effetto firmare condizioni di contratto, dalle quali si desume che poco viene fatto a protezione dei nostri dati. Inoltre, se il consenso da fornire deve essere il frutto di una scelta informata, molto lavoro dovrà essere fatto per rendere alcune informative compliance alla normativa privacy[12].

4. La tutela della privacy nei servizi delle *insutech*

I principali dati che le auto di ultima generazione memorizzano variano: dalle diverse modalità di guida da parte del conducente, alla tensione delle cinture di sicurezza, dal numero dei viaggi fatti, a quello dei chilometri percorsi e alle ultime destinazioni inserite nel sistema di navigazione. Sul fronte della manutenzione la vettura ha raccolto informazioni sui giri del motore, il chilometraggio del veicolo e lo stato delle luci. Per non parlare dei dati generati dalla sincronizzazione con lo smartphone. Questa mole di dati da una parte, potrebbe essere utile alla casa costruttrice per creare esperienze di viaggio sempre più confortevoli e tecnologicamente all'avanguardia grazie agli immancabili sistemi di infotainment (ma anche per supportare e facilitare le attività di manutenzione e/o diagnostica) e, dall'altra, fanno gola soprattutto al comparto assicurativo, che ha già da tempo individuato nella *usage-based insuran-*

[11] N.H.T.S.A., *Guidance and Recommended Best Practices: Safety-Related Defects, Unreasonable Risk, and Automated Safety Technologies*, su www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/final_enforcement_guidance_bulletin.pdf;
Sul punto Cfr., R. Thibadeau, *The Need for Data-at-Rest in Storage Device Privacy in V2V and V2I Communications*, www.ftc.gov/system/files/documents/publiccomments/2017/04/00014-140528.pdf

[12] Sull'importanza del ruolo del consenso quale forma di esercizio del diritto del singolo alla protezione dei dati personali Cfr, L.Gatt, R.Montanari, I.A. Caggiano, *Consenso al trattamento dei dati personali e analisi giuridico comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali,* in *Pol. Dir.*2/2017, pp. 343-360.

ce (UBI) la naturale evoluzione delle proposte RC auto. Il motivo è molto semplice. Posto che il contratto di assicurazione prevede per sua stessa natura la valutazione di alcuni parametri soggettivi riguardanti il cliente, una maggiore conoscenza dell'effettivo utilizzo del veicolo e il monitoraggio dello stile di guida aiutano a customizzare l'offerta in modo più efficiente. Negli ultimi anni diverse assicurazioni hanno inserito a listino offerte di *usage-based insurance* (UBI), non solo nella formula Pay per Use o Pay as You Drive (premio tarato sull'effettivo utilizzo chilometrico del veicolo) ma, anche, nella formula Pay How You Drive (PHYD), ossia con criteri che prendono in considerazione abitudini e condotte del conducente. L'implementazione del modello PHYD ha principalmente eletto in un'apposita black box (da installare sulla propria auto) il *device* deputato a riportare informazioni in tempo reale alla compagnia. La black box assicurativa, nella sua versione standard, è un dispositivo satellitare dotato di un geo-localizzatore (utile anche in caso di furto) e di un accelerometro in grado di registrare tutti i movimenti del veicolo; il tutto connesso ad una centrale remota, in genere tramite una SIM card inserita nella scatola. Ai fini dell'aggiornamento del premio, i dati più rilevanti scaturenti dalla black box sono il chilometraggio medio (effettivo utilizzo), le zone frequentate (aree a rischio o meno), lo stile di guida (ad es. velocità, modo di accelerare/frenare), eventuali informazioni utili a riscostruire la dinamica di un sinistro (un bel deterrente anti-frode, oltre che dati utili per accertare responsabilità)[13].

Siamo sicuri che la black box debba registrare necessariamente tutti questi dati? Ovviamente no. Dipende dall'utilizzo che il consumatore vuole farne. Se si valuta un guidatore esperto che non ha mai causato sinistri per la sua guida prudente, ma che vive in una zona ad alta intensità criminale, potrà decidere di applicare la scatola solo ed esclusivamente per avere maggiori probabilità di ritrovare il veicolo in caso di furto. Da qui l'importanza per i costruttori di *disegnare* un dispositivo "duttile", che sia in grado di registrare solo quei dati (coordinate gps e percorsi effettuati) utili al ritrovamento della

[13] M. Massimini, *Sarà lo smartphone ad informare l'assicurazione sul tuo stile di guida*, 2018, reperibile in https://www.privacy.it/2018/12/12/smartphone-sensore-assicurazione-auto/. Per una analisi più critica e dal respiro internazionale Cfr. R. Herold, C. Hertzog, *Data privacy for the smart grid*, Crc Press, 2015.

vettura ma, anche, di essere facilmente configurato dall'installatore per recepire ulteriori informazioni nel caso in cui l'assicurato abbia sottoscritto ulteriori servizi, come vedremo a breve. Nell'informativa che l'interessato firmerà troveremo i seguenti dati: i suoi dati anagrafici, dati relativi al veicolo assicurato, dati di polizza, dati relativi alla localizzazione e, più in generale, alla geo-referenziazione del veicolo. Non vi è dubbio che il conferimento dei dati sopracitati sarà obbligatorio, in quanto funzionali all'esecuzione del contratto[14]. L'esempio di cui sopra è ovviamente un caso limite. È chiaro che, una volta installata la box, la maggior parte degli assicurati vorrà usufruire di sconti sul premio della polizza Rca, e, dunque, si aggiungeranno altri dati che saranno trattati e che dovranno essere tutti ben chiaramente definiti nell'informativa come, ad esempio, i dati comportamentali relativi all'uso del veicolo in base a parametri di tempo e luogo, nonché indicatori di guida funzionali alla valutazione dello stile di guida dell'Interessato (c.d. driving behaviour) quali: velocità, cambi di direzione improvvisi, dati relativi alla rilevazione delle accelerazioni e delle decelerazioni del veicolo, fondamentali soprattutto nel ricostruire la reale dinamica dei sinistri.

A questo punto pochi dubbi ci sono sul fatto che, grazie a questi dati, verrà posta in essere un'attività di profilazione che potrà essere propedeutica ad un processo decisionale automatizzato (ovvero a decisioni basate unicamente sul trattamento automatizzato ex art.22 del regolamento europeo 2016/679). Infatti, il regolamento europeo definisce la profilazione all'articolo 4, punto 4, come: ‹‹*qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi,* ***l'affidabilità, il comportamen-***

[14] Di solito il cliente firma la polizza assicurativa rca auto tramite la sua assicurazione, la quale avendo siglato una partnership con la società di servizi telematici, sottoporrà in quella sede anche il contratto e la relativa informativa privacy per l'istallazione della black box. In realtà, le case automobilistiche stanno istallando questi dispositivi su tutti i nuovi modelli così facendo, non solo acquisiscono un peso notevole nell'eventuale cessione dei dati alle assicurazioni ma, in un futuro nemmeno così lontano, una volta acquisite le tecniche di analisi dei dati, avranno tutti gli strumenti per fornire in prima persona le opportune coperture assicurative.

to, l'ubicazione o gli spostamenti di detta persona fisica››.[grassetto aggiunto]

Non solo. Come afferma il Gruppo di lavoro art.29 (di seguito WP29) nelle linee guida sulla profilazione e sul processo decisionale automatizzato, quest'ultimo ‹‹*ha una portata diversa da quella della profilazione, a cui può sovrapporsi parzialmente o da cui può derivare. Il processo decisionale esclusivamente automatizzato consiste nella capacità di prendere decisioni impiegando mezzi tecnologici senza coinvolgimento umano. Le decisioni automatizzate possono essere basate su qualsiasi tipo di dati, ad esempio dati osservati riguardo a una persona (come i dati relativi all'ubicazione raccolti tramite un'applicazione*)››[15]. Ovvero, come nel caso di specie, da un dispositivo satellitare.

Per questo motivo (e non solo) le attività di profilazione e tutti i processi decisionali automatizzati che comportano l'uso di dati personali, dovranno essere permeati dai principi in materia di protezione dei dati e, dunque, giammai in grado di creare situazioni inique e/o discriminatorie. Il principio cardine che il titolare del trattamento dovrebbe seguire come un mantra − data la complessità degli algoritmi utilizzati − è rappresentato dalla trasparenza del trattamento, che gli impone di fornire agli interessati informazioni concise, trasparenti, intelligibili e facilmente accessibili sul trattamento dei loro dati personali. Il settore bisognoso di una concreta e piena applicazione di questo fondamentale principio, preso come esempio dal Gruppo di lavoro art.29, è proprio quello assicurativo, considerata la diffusa strategia commerciale degli assicuratori di offrire tariffe e servizi assicurativi in base al comportamento di guida delle persone, proprio grazie alla raccolta ed utilizzo

[15] Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679 (WP251), del 3/10/ 2017. Versione emendata e adottata in data 6 febbraio 2018, pg 8, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053
Particolarmente significativo, per un completo excursus normativo, giurisprudenziale, dottrinale dell'istituto della profilazione, il contributo di M. Siano, L. Montuori, *Evoluzione del concetto di consenso informato nel mondo digitale e transizione del marketing tradizionale alle attuali sfide della profilazione*, in G. Busia, L. Liguori, O. Pollicino (a cura di), *Le nuove frontiere della privacy nelle tecnologie digitali. Bilanci e prospettive.,* Roma, 2016, pg 114 ss.

delle informazioni di cui sopra per fini di profilazione con l'obiettivo di individuare comportamenti di guida errati[16].

Svolgere queste attività sulla base della condizione di liceità rinvenibile nell'art 6 lett.b. del GDPR (‹‹*il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso*››) è molto importante, dal momento che quest'ultima rappresenta una delle tre eccezioni al divieto generale all'adozione di un processo decisionale unicamente automatizzato, che produce effetti giuridici che riguardano l'interessato o che incida in modo analogo significativamente sulla sua persona. Non solo. Come afferma il WP29, la profilazione è consentita se è necessaria ai fini degli interessi legittimi perseguiti dal titolare del trattamento o da un terzo. Questi sussisterebbero, in virtù del considerando 47 del regolamento europeo, quando il trattamento dei dati personali è strettamente necessario a fini di prevenzione delle frodi. Quale comparto, se non quello assicurativo, ha questa primaria necessità, basti pensare che l'intento originario di questi dispositivi era proprio quello di smascherare falsi sinistri. Pertanto, a ben vedere, si pone in essere un trattamento lecito per una finalità che il cliente/interessato ragionevolmente può attendersi.

Dunque, fin qui nulla quaestio. Tuttavia se si considera che il titolare del trattamento deve inoltre fornire all'interessato informazioni sui dati raccolti e, se del caso, sull'esistenza di processi decisionali automatizzati di cui all'articolo 22, paragrafi 1 e 4, sulla logica applicata, nonché sulla rilevanza e sulle conseguenze previste di tale trattamento, ecco che arrivano le prime

[16] C'è da sottolineare che l'uso massiccio di questi dispositivi, che vede l'Italia il maggior fruitore a livello mondiale, è anche frutto di una frastagliata produzione normativa. Sul punto si rinvia a T. Pertot, *L'assicurazione auto con scatola nera. Sconti tariffari vs dati personali*, in *ODCC*, fasc.2, dicembre 2018, pg 544 ss. Dopo aver egregiamente analizzato il complesso iter legislativo per l'utilizzo di tali dispositivi, una volta suffragata la tesi della negoziabilità dei dati utilizzabili quale mezzo di pagamento al pari del denaro all'interno di rapporti sinallagmatici, l'autore sostiene che sarebbe stata auspicabile una maggiore audacia da parte del nostro legislatore, che poteva approfittare dell'approvazione della Legge Concorrenza per regolare in maniera più incisiva una prassi (quella consistente nell'utilizzazione dei dati quale strumento di scambio per ottenere un bene o servizio) che, diffusa con particolare riguardo alla fornitura di contenuti e servizi digitali in rete, ricorre oggi anche in ambito assicurativo.

note dolenti. Il motivo è da rinvenire nelle informative attualmente predisposte dalle società di servizi telematici e dalle assicurazioni che peccano molto in termini di chiarezza[17].

In particolar modo, uno degli aspetti che meriterebbe una maggiore intelligibilità, riguarda l'individuazione dei dati, delle finalità e delle modalità con le quali essi sono ceduti a terzi. In effetti molti di noi – più o meno consapevolmente − mostrano un po' di ritrosia a firmare documenti in cui si menziona a questa evenienza e, dunque, non è peregrino chiedersi se il dato profilato ceduto (*rectius* venduto) a terzi operanti in tutt'altro settore commerciale (in primis finanziario e telecomunicazioni), produca rischi maggiori per la nostra privacy.

In questo contesto, è chiaro che i contitolari non stanno utilizzando le risultanze della profilazione per le finalità di meglio individuare un equo premio alla base del contratto Rca quanto, piuttosto, stanno offrendo un modello profilato dal quale altre aziende possono trarre notevoli vantaggi in termini soprattutto di marketing, motivo per cui, la condizione di legittimità − in questa fase − deve traslare dalla necessità di eseguire un contratto (o interesse legittimo a tutela contro eventuali frodi) a quello del consenso esplicito ex art 22 par 2 lett.c. del GDPR. Non solo. Se si effettua una profilazione rispettosa degli articoli13 e 14*,* un intermediario di dati dovrà informare l'interessato in merito al trattamento e al fatto che intende condividere il profilo con altre organizzazioni. Deve inoltre indicare separatamente anche i dettagli relativi al diritto di opposizione di cui all'articolo 21[18].

---

[17] Per un approfondimento nel comprendere se, in un simile scenario, il consenso al trattamento dei dati personali possa essere realmente uno strumento di tutela funzionale al perseguimento dei fini stabiliti dall'attuale normativa europea in materia, Cfr: M.C. Gaeta, *La protezione dei dati personali dell'Internet of Things: l'esempio dei veicoli autonomi,* in *Dir. Inform*., n.1, 2018, pg 147-178; E.C.Pallone, *Internet of Things" e l'importanza del diritto alla privacy tra opportunità e rischi*, in *Cibersp. dir,* n. 1-2 2016, pp. 163-183.

[18] Sul tema Cfr., P. Pacileo, *Profilazione e diritto di opposizione*, in S. Sica, V. D'Antonio e M.G.Riccio (a cura di*), La nuova disciplina europea della privacy*, Milano, 2016, pg. 177 ss.; A. Ricci, *I diritti dell'interessato*, in G. Finocchiaro (diretto da), Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali, Bologna, 2017, pg 235.

In realtà proseguendo nel parere del wp29 si evince che le informazioni che devono essere rese non terminano qui, infatti, l'impresa deve informare l'interessato [articolo 14, pa-

Aggiungerei che, nel novero delle informazioni da menzionare, non devono assumere un ruolo di secondo piano (come a volte accade) quelle inerenti il periodo di conservazione dei dati. Più precisamente, sarebbe auspicabile una chiara e ragionevole correlazione tra la tipologia di dato raccolto, la sua finalità e la corretta indicazione del periodo di retention. In virtù di quanto finora affermato si evince chiaramente che, seguire pedissequamente i preziosi consigli del parere WP251, ridurrebbe drasticamente le minacce alla nostra privacy nel settore delle assicurazioni tecnologiche.

5. *Smart road* e privacy: ancora qualche criticità.

Finora l'analisi si è focalizzata sulle applicazioni dell'IoT all'interno della vettura e sulle ripercussioni che esse hanno sulla nostra sfera privata. Adesso l'attenzione sarà diretta su un altro ambito, quello dell'interazione tra veicoli (vehicle-to-vehicle V2V) e tra questi e le piattaforme tecnologiche, che renderanno le nostre infrastrutture viarie, di fatto, delle "*smart road*" (Vehicle-to-infrastructure V2I). È un settore connotato da una elevata complessità, che richiederebbe conoscenze scientifico-tecnologiche non riassumibili di certo in un paragrafo, in ogni modo accennerò − per sommi capi − ad alcuni dei principali aspetti tecnici che sono alla base di queste comunicazioni anche se, il perno fondamentale della trattazione, verterà su una analisi critica del parere del WP29 03/2017, adottato il 4 ottobre 2017, di cui è relatore il garante italiano[19]. Ma procediamo con ordine.

Una delle ragioni alla base della spasmodica e incessante attività dell'ingegneria automobilistica di dotare le vetture con un sempre maggior

---

ragrafo 1, lettera c)] in merito alle finalità dell'utilizzo del profilo e alla fonte da cui ha ottenuto l'informazione [articolo 14, paragrafo 2, lettera f)] L'intermediario di dati e l'impresa devono consentire all'interessato di accedere alle informazioni utilizzate (articolo 15) per correggere eventuali informazioni errate (articolo 16) e, in determinate circostanze, di cancellare il profilo o i dati personali utilizzati per crearlo (articolo 17). L'interessato deve inoltre ricevere informazioni sul proprio profilo, ad esempio, in merito ai "segmenti" o alle "categorie" nei quali viene collocato.

[19] Gruppo di lavoro ex art. 29, *Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport System (C-ITS)*- WP252-, adottate il 04/10/2017, reperibile in https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610171

numero di sensori interni ed esterni, è da rinvenire nella direttiva 2010/40/UE1 che promuove lo sviluppo di tecnologie di trasporto innovative, per creare sistemi di trasporto intelligenti (ITS), grazie all'introduzione di standard e specifiche comuni in tutto il territorio dell'Unione Europea[20]. Se a ciò si aggiungono le dichiarazioni della commissaria Ue ai Trasporti Violeta Bulc, durante la presentazione delle linee guida del piano Cooperative Intelligent Transport Systems (C-ITS), secondo la quale la digitalizzazione del trasporto non è un'opzione ma una necessità, con investimenti iniziali che supereranno i tre miliardi di euro, il quadro normativo-tecnologico in cui ci muoviamo è più chiaro.

La piattaforma C-ITS è un progetto della Commissione europea nato con l´obiettivo di migliorare la sicurezza stradale, l'efficienza del traffico, il comfort di guida e di ridurre le emissioni inquinanti, aiutando l'automobilista a prendere le decisioni più opportune al verificarsi di determinati eventi esterni (ingorghi, incidenti stradali, condizioni metereologiche, lavori in corso). In breve, lo scopo è di avere infrastrutture che interagiscano con gli automobilisti con il primario obiettivo di offrire un viaggio sicuro, confortevole e col minor impatto ambientale. Finalità importantissime che saranno perseguite nel momento in cui verranno costruiti, nel rispetto di una *privacy e security by design*, enormi data base che dovranno raccogliere una

[20] Per una interessante analisi del percorso giuridico e tecnologico per la creazione delle smart road: Ministero delle Infrastrutture e dei Trasporti, *Standard funzionali per le smart-road reperibile* su http://www.mit.gov.it/sites/default/files/media/notizia/201606/Standard%20funzionali%20per%20le%20Smart%20Road.pdf; Per analizzare e capire il funzionamento di alcuni di questi sensori Cfr., M. Muek, I.Karis, *Networking Vehicles to Everything: Evolving Automotive Solutions,* Walter de Gruyter Inc, Boston-Belin, 2018. The current road traffic act and safety related use cases do not make use of V2X networking and connectivity so far. But these use cases will evolve. Millions of vehicles have been equipped with emergency call services for years providing a wireless link into the vehicle. Typical additional use cases of these V21 application are emergency electronical brake light (EEBL), forward collision warning (FCW), intersection collision warning (ICW), stationary vehicle warning (SVW) and pre-crash-warning (PCW). We find in the vehicle automatic high beams, forward collision warning, front automated emergency braking, lane departure warning, lane keeping assist, blind-spot monitor, front parking assist, parking assist, rear automated emergency braking, rear cross-traffic monitor, rear parking assist, automatic distance control (ADC), blind spot sensor, lane assist, light assist, dynamic light assist, drowsiness warning, side assist, traffic sign recognition and traffic jam warning (TIW).

mole inimmaginabile di dati inviati da una moltitudine di sensori presenti non solo sulle auto ma, anche, sui semafori (che consentiranno in real time una gestione intelligente del traffico), nella segnaletica stradale, così come sull'illuminazione pubblica (diminuendo l'intensità della luce in assenza di pedoni e automobili).

In tema di sicurezza, quello della Smart Mobility e delle Smart Road si intreccia fortemente con il sistema delle emergenze e la realizzazione delle reti PPDR (*Public Protection and Disaster Relief*): si tratta di reti radio a banda larga progettate per poter rispondere all'esigenza di un'infrastruttura radio efficiente, in grado di supportare le operazioni di soccorso su vasta scala, che possano derivare da eventi emergenziali di qualunque tipo, sia di tipo naturale (per es. vaste inondazioni, incendi, frane ecc.) che legati ad attività umane (per es. di matrice terroristica ecc.)[21].

Gli indubbi benefici dell'ITS si scontrano, tuttavia, con un quadro normativo che appare inadeguato e con una scarsa consapevolezza delle istituzioni, incapaci ancora di affrontare in modo sinergico sia le problematiche giuridiche che quelle più prettamente tecniche legate, ad esempio, ai necessari processi di standardizzazione, che debbono garantire architetture scalabili, sicure, interoperabili e nello stesso tempo flessibili, come richiesto dalla continua innovazione, in modo tale da consentire a tutti i veicoli di dialogare tra

[21] Per ulteriori approfondimenti: D. Proto, *Sicurezza delle auto connesse: le sfide delle regole in Italia,* su https://www.agendadigitale.eu/smart-city/sicurezza-delle-auto-connesse-le-sfide-e-gli-scenari-normativi-in-italia/ "…Le operazioni di protezione civile e/o di pubblico soccorso utilizzano in modo pesante l'accesso ai dati distribuiti sui database delle organizzazioni coinvolte nella gestione delle emergenze – come la polizia, i vigili del fuoco, la protezione civile (nelle sue declinazioni centrali e regionali) e l'emergenza sanitaria. Le reti PPDR devono essere in grado di gestire volumi elevati di scambio dati in modo sicuro: queste informazioni comprendono, infatti, immagini e mappe provenienti dalla fonti più disparate. Allo stesso modo il flusso di informazioni di ritorno da unità in campo per i centri di controllo operativi dovrà essere trattato con analoga priorità: durante una situazione di emergenza, le Autorità responsabili del soccorso sono tenute a prendere decisioni che sono indubbiamente influenzate dalla qualità e dalla tempestività delle informazioni ricevute e sotto tale aspetto forse si rendono nel breve periodo necessarie delle scelte, considerando quanto previsto da un lato dai Report 53 e 60 della Cept e dalla decisione europea 2016/687 in relazione alla banda 700 Mhz e dall'altro dalla legge di stabilità per l'anno 2018. Alcune sezioni del lavoro illustrano, in maniera tecnica, come avverranno le comunicazioni delle connected car attraverso il sistema DSRC

di loro e con i diversi sistemi a bordo strada o con i diversi centri servizi, senza soluzione di continuità[22]. Come affermato in precedenza, in questo scenario tecnico-giuridico non ancora così maturo, il parere del WP29 è fondamentale per avere una visione più chiara di questo ecosistema tecnologico e, di conseguenza, per poter verificare se vengono alla luce minacce per la nostra privacy.

Partendo dalla fine del parere incontriamo tutte le azioni che, secondo il Gruppo di lavoro art.29, bisogna porre in essere per raggiungere il duplice, possibile obiettivo dello sviluppo tecnologico e della tutela dei diritti. Queste raccomandazioni sono state ribadite, in una sorta di decalogo, nel corso dell'assemblea dello European Telecommunications Standards Institute (ETSI) che è l'organo di standardizzazione che, a livello continentale, sta sviluppando le architetture e i protocolli per lo scambio delle informazioni tra veicoli[23].

Dal mix di questi due importanti documenti è possibile rinvenire apprezzabili considerazioni, che non possono non essere condivise quali: garantire la qualità dei messaggi rivolti ai guidatori, in modo che non si generino falsi allarmi o che, al contrario, situazioni di reale pericolo non siano prontamente individuate e rese note; certificare i dispositivi e i certificatori, in modo da impedire l'ingresso nel sistema di dispositivi e soggetti che possano trasmettere messaggi falsi o di disturbo ai veicoli circostanti; la necessità di predisporre una valutazione di impatto sulla protezione dei dati per determinare, l'origine, la natura, la particolarità e la gravità di un rischio elevato per i diritti e le libertà delle persone fisiche.

In alcuni punti del parere ci sono anche considerazioni che meriterebbero di essere analizzate più approfonditamente, ad esempio quando si afferma che bisogna riconoscere che i messaggi scambiati tra veicoli e quelli con le

[22] D. Proto, *Sicurezza delle auto connesse, Mise: "Ecco i nodi normativi da sciogliere",* https://www.agendadigitale.eu/infrastrutture/mise-auto-connesse-e-sicurezza-ecco-i-nodi-regolamentari-da-sciogliere/. D'altronde già S. Rodotà riteneva che le regole giuridiche si devono adattare al ritmo veloce del cambiamento tecnologico, in *Tecnologie dell'informazione e frontiere del sistema sociopolitico*, Pol. dir., 1982, pp.25 ss.

[23] G. D'Acquisto, *Sistemi di trasporto intelligenti e protezione dei dati personali, come fare*; https://www.agendadigitale.eu/smart-city/sistemi-di-trasporto-intelligenti-e-protezione-dei-dati-personali-come-fare/

infrastrutture di trasporto intelligente (segnaletica stradale, stazioni fisse di rilevamento) sono dati personali, visto il forte potere identificativo dei dati di localizzazione, oppure quando si dedica particolare attenzione a scongiurare l'impiego eventuale del C-ITS come strumento per ‹‹*pedinare*›› a distanza le persone. Prima di confutarle parzialmente, è necessario capire − succintamente − cosa (e come) viene scambiato nell'C-ITS.

Nel parere il WP29 illustra che sono due le tipologie di messaggi che vengono scambiati nell'ambito del C-ITS: i c.d. messaggi CAM (Cooperative Awareness Messages) trasmessi con continuità e contenenti dati cinematici oltre alle dimensioni del veicolo, e i messaggi DENM (Decentralised Environmental Notification Messages) cioè messaggi decentrati di notifica ambientale inviati in aggiunta ai messaggi CAM solo al verificarsi di eventi specifici (come ad esempio incidenti) per situazioni di emergenza urgenti e contengono informazioni sull'evento. I messaggi CAM e DENM prevedono la firma crittografata, che garantisce alla parte ricevente che i messaggi sono stati inviati da un mittente affidabile.

L'aspetto più interessante si rinviene quando Il gruppo di lavoro del C-ITS ha rilevato correttamente che i dati trasmessi tramite il C-ITS sono dati personali in quanto si riferiscono agli interessati identificati o identificabili. Gli interessati possono essere identificati in vari modi. Innanzitutto, mediante i certificati ottenuti dall'infrastruttura pubblica PKI, in quanto tali certificati saranno unici fin dalla progettazione, al fine di distinguere inequivocabilmente il veicolo in cui sono installati. Secondariamente, mediante i dati relativi all'ubicazione, poiché è nota la loro capacità di identificazione: bastano pochi punti in un percorso per distinguere con estrema precisione un individuo in una popolazione, tenendo conto dei modelli di mobilità generalmente regolari delle persone. Ma è proprio così? Non vi è ombra di dubbio che le informazioni collegate con dati personali, che permettono l'identificabilità di un soggetto, siano a loro volta qualificati come dati personali[24]. Ma questo processo non è così facile come si potrebbe immaginare.

[24] Sui concetti di identificativo, identificazione e identificabilità Cfr., L. Bolognini, E. Pellino, C. Bistolfi, *Il regolamento privacy europeo, commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016, pg 50 ss; G Finocchiaro, *Privacy e protezione dei dati personali*, Bologna, 2012, 48 ss

Durante la ricerca e analisi della documentazione per la realizzazione di questo articolo, l'attenzione è ricaduta su una semplice quanto intuitiva iconografia di un documento del ministero dei trasporti americano[25] che mostra come, sebbene i veicoli siano provvisti di targa e ID − che conducono ad una facile identificabilità del proprietario − in realtà, non sono questi i dati che vengono materialmente scambiati con le altre vetture e le piattaforme tecnologiche stradali. Ciò che è oggetto di scambio è, piuttosto, la velocità, la distanza, lo stato dell'impianto frenante ecc. In realtà, non bisogna andare così lontano per capire che il processo che porta all'identificazione di un individuo sulla base di quei dati effettivamente scambiati (soprattutto in ambito V2V), non sia così semplice. Difatti, basterebbe recuperare informazioni sul funzionamento del cosiddetto sistema *e-call* per comprendere che, in ottemperanza alla normativa privacy – in particolar modo dei principi di minimizzazione della raccolta dei dati e della privacy by design – ciò che viene raccolto dalle centrali di soccorso attraverso l'MSD (minum set of data) sono: il tempo, la posizione, la marca, il modello della vettura e null'altro. Solo dopo la ricezione di queste informazioni potrebbe intercorrere una reale telefonata tra soccorritore e guidatore, per capire le sue effettive condizioni[26].

Invece, riguardo i problemi relativi alla localizzazione, è lo stesso WP29 a fornire una strategia per limitare il rischio di un eccessivo e continuato monitoraggio (peraltro da tempo avallata dalla comunità scientifica) vale a dire, la localizzazione a corto raggio. Quest'ultima realizzerebbe una stretta connessione causale fra la viabilità stradale e i veicoli che si spostano nella zona in questione, ed è quindi considerata necessaria per attivare il sistema e per poter interagire con le applicazioni. Al fine di evitare la localizzazione prolungata, che non è essenziale ai fini della sicurezza stradale, i titoli di au-

[25] U.S. Department of Transportation, *National Strategy for Transportation DataThe Future of Intelligent Transportation Systems*, 2017, https://www.its.dot.gov/presentations/sxsw/SXSW2017_ITS_Data.pdf

[26] M. Planamante, *Smart Cars: how the Internet of Things is enabling new business models in the automotive industry*, 2016, pg 56, reperibile in https://www.politesi.polimi.it/handle/10589/131346; Ai sensi degli artt. 4 e 6, Reg. 2015/758/UE, il sistema è attualmente obbligatorio e, quindi, non è richiesto il consenso i dati personali sono conservati dal fornitore del servizio eCall — titolare del trattamento — solo per il periodo di tempo necessario ad affrontare le situazioni di emergenza e vengono cancellati completamente appena non sono più necessari

torizzazione (così come gli pseudonimi) devono essere modificati frequentemente[27].

Ad avviso dello scrivente, il punto più enigmatico del parere riguarda la corretta individuazione della base giuridica del trattamento. Il WP29 suggerisce che, per un trattamento di dati di questa portata, posto in essere per migliorare la sicurezza stradale − a maggior ragione con l'avvento degli automobili a guida automatica − si debba rinvenire la base giuridica nell'articolo 6, paragrafo 1, lettera c), del GDPR (*il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento*). A questo punto, la Commissione dovrà vagliare al più presto questa soluzione, per poi avviare un iter legislativo per evitare che il trattamento dei dati relativi all'ubicazione e di altri dati personali dei cittadini dell'UE all'interno del C-ITS, avvenga senza il fondamento di una base giuridica e non sia tutelato interamente da un adeguato livello di protezione.

Quindi, problema subito risolto. Invece no. La ricerca della corretta individuazione della condizione di liceità del trattamento diventa molto complessa, nel momento in cui il Gruppo di lavoro art.29, dovendo confutare alcune soluzioni prospettate dalla commissione di lavoro C-ITS, avvia un fra-

[27] Secondo A. Falaschi, ‹‹*per migliorare la difesa della privacy il cambio di pseudonimo dovrebbe avvenire in contemporanea per tutti i nodi in una stessa zona, meglio ancora se in corrispondenza di incroci e svincoli*››, *Vehicular Ad Hoc Networks, Dicembre 2009*, http://infocom.uniroma1.it/alef/seminario_vanet.pdf;
Per una disamina più approfondita Cfr., AA.VV, *Security and Privacy for Next-generation Wireless Networks*, Springer, 2018, pg 111 ss, *Pseudonym-based privacy protection schemes are commonly accepted schemes in the VANET. A vehicle can often use a pseudonym to hide its identity while moving. However, if the timing of the vehicle's pseudonym-changing is not appropriate (for example, only one car converts a pseudonym at a certain time), it will be easy for an attacker to trace its true identity information. There are two main ways to solve the pseudonym/vehicle connection problem: mix zones and silent periods. A mix zone is a predetermined area and is usually chosen where there is heavy traffic flow. After the vehicle enters the area, it changes its pseudonym (35). There is a large spatial gap between the last beacon signal sent with the old pseudonym and the first one sent with the new pseudonym, and as a result, these two data sets are not easily connected, which effectively cuts off the connection between the vehicle and the two pseudonyms.* Gli autori, inoltre, spiegano come il livello di sicurezza di questo tipo di informazioni sia molto elevato attraverso l'utilizzo della crittografia ad anello, la cui applicazione in questo campo si sta sempre più diffondendo con ottimi risultati.

stagliato percorso argomentativo. Infatti, sebbene in un primo momento afferma che ‹‹*la funzione centrale del C-ITS è costituita dal rilevamento dell'ubicazione, della velocità e della direzione dei veicoli* [e che] q*uanto maggiore è la frequenza dei messaggi scambiati, tanto più nitida e più dettagliata è la panoramica dei veicoli dell'ambiente circostante e maggiore la capacità di previsione dei pericoli del sistema*[...]; *il livello di adozione e di conferimento dei dati sia un fattore cruciale per il funzionamento del C-ITS: un contributo di dati insufficiente o una bassa risoluzione della vista ambientale catturata da ogni veicolo potrebbe compromettere o persino rovinare la validità del C-ITS in quanto strumento per la sicurezza stradale*››, successivamente − glissando anche su quei suggerimenti che esso stesso fornisce per la limitazione dei rischi derivanti da una localizzazione meticolosa − asserisce che ‹‹*incitare i conducenti ad adottare il sistema C-ITS non significa instaurare con la forza un sistema invasivo di localizzazione. La possibilità di beneficiare del C-ITS di per sé dovrebbe incentivare i conducenti ad aderire liberamente al C-ITS. In questo modo sarebbe possibile raggiungere in modo naturale una massa critica di utenti affinché il sistema funzioni correttamente senza alcuna imposizione; al tempo stesso, si lascerebbe alle persone la libertà di scegliere se desiderano partecipare al sistema e, in caso affermativo, di selezionare le opzioni di localizzazione (tempi, frequenza, luoghi) che meglio si confanno alle rispettive preferenze*››[28]. Più facile a dirsi che a farsi. In realtà, è ancora lo stesso WP29 a riconoscerlo quando afferma che ‹‹Il gruppo di lavoro del C-ITS non trova il giusto equilibrio tra la necessità di promuovere l'adozione del C-ITS e quella di prevenire i comportamenti parassitari – conducenti che non partecipano al sistema ma godono dei suoi benefici. Non solo. È inevitabile chiedersi che senso avrebbe un C-ITS nel momento in cui un soggetto, avendo la possibilità di scegliere se avvalersene o oppure no, opti per quest'ultima soluzione.

Era lecito attendersi dal parere un maggiore proattività e risolutezza nel dirimere concretamente le problematiche della ricerca della condizione di liceità che la commissione di lavoro ITS non riesce a risolvere, e non solo scartare – seppur con argomentazioni giuridiche condivisibili – le varie al-

[28] Op. cit., pg 10 ss.

ternative proposte[29]. Ad esempio, si poteva approfondire − piuttosto che sorvolare − la lettura in combinato disposto dell'art 23 del regolamento 2016/679 e del connesso considerando 73, in virtù del quale "*Il diritto dell'Unione o degli Stati membri può imporre limitazioni a specifici principi e ai diritti[…]ove ciò sia necessario e proporzionato in una società democratica per la salvaguardia della sicurezza pubblica, ivi comprese la tutela della vita umana, in particolare in risposta a catastrofi di origine naturale o umana*, *per la tutela di altri importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro"*. Evitare oltre 25.000 morti all'anno in Europa per incidenti stradali, potrebbe essere uno di questi obiettivi. In questo modo, si sarebbe ulteriormente avallata la principale scelta di rinvenire la condizione di liceità nell' art 6. par.1 lett. c. Così facendo, la commissione C-ITS avrebbe avuto idee più chiare in merito, scongiurando un impasse giuridico che rischia di produrre un preoccupante rallentamento dello sviluppo di questa tecnologia.

6. Conclusioni

Mentre ero alle prese con le considerazioni finali di questo contributo, sui principali network informativi rimbalzava la notizia che l'industria automobilistica registrava l'ennesimo calo di vendite, con inevitabili gravi ripercussioni sui gruppi quotati. Per fronteggiare un mercato da tempo instabile e

[29] In riferimento alle considerazioni elaborate per rigettare i vari tentativi di rinvenire altre condizioni liceità, non si possono non condividere le seguenti argomentazioni rinvenibili a pg 12 del parere Innanzitutto, *è importante determinare chiaramente in anticipo le parti coinvolte nel contratto, al fine di limitare il trattamento nel ristretto perimetro dei soli soggetti coinvolti nell'ambito di applicazione del C-ITS ed evitare qualsiasi ulteriore utilizzo dei dati ad opera di altre parti sconosciute; In merito all'eventuale applicazione della necessità di trattare i dati per un interesse legittimo (articolo 6, paragrafo1, lettera f), del GDPR;* il Gruppo di lavoro Articolo 29 rammenta che *questa non dovrebbe essere considerata come "l'ultima spiaggia" per casi complessi nei quali è difficile applicare altre basi giuridiche che giustifichino la liceità del trattamento. L'esito di una verifica potrebbe determinare se l'articolo 6, paragrafo 1, lettera f), del GDPR può essere preso a fondamento per il trattamento. L'identificazione dei titolari del trattamento e dei loro interessi costituisce una condizione preliminare necessaria, come affermato nel documento*.

con una produzione destinata nei prossimi anni a ridursi, le scelte commerciali dei produttori di auto sono sempre più focalizzate sulla capacità di ottenere introiti attraverso una serie di servizi che possono offrire grazie ai sistemi di infotainment e allo sviluppo dei sensori funzionali alla comunicazione V2X (vehicle to everything). Sulla scia di quanto finora sostenuto verrebbe da dire che c'è poco da stare allegri, sia per la sicurezza dei nostri dati (sul versante della *security e privacy by design*) sia sulla effettiva comprensione delle finalità e modalità del trattamento, per non parlare della difficoltà di individuare chi rivestirà il ruolo di titolare del trattamento, specialmente nel settore delle smart road. Infatti, da una parte c'è il C-ITS le cui piattaforme tecnologiche dovranno dialogare con sensori sviluppati e prodotti dalle case automobilistiche, dall'altra il settore automotive che vuole ottenere profitti proprio dal loro utilizzo. Un timido e apprezzabile intervento legislativo, in questo scenario ipertecnologico, si è realizzato con il decreto del Ministero delle Infrastrutture e dei Trasporti del febbraio del 2018 che fissa le prime regole − in particolar modo − per i test e lo sviluppo delle auto a guida autonoma. Tuttavia, sarebbe auspicabile un nuovo provvedimento che si focalizzi, non solo sulla complicata scelta e le relative conseguenze connesse all'individuazione della condizione di liceità del trattamento dei dati effettuato con le comunicazioni V2I, ma che sia anche capace di dirimere sul nascere quelle problematiche economico-giuridiche che inevitabilmente sono destinate a sorgere tra player pubblici e privati.

Diritto Mercato Tecnologia

Numeri Speciali

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

2017 Il Mercato Unico Digitale
a cura di Gianluca Contaldi

2018 La Ricerca su Materiali Biologici di Origine Umana:
Giuristi e Scienziati a confronto
a cura di Alberto M. Gambino, Carlo Petrini e Giorgio Resta

2019 La Tassazione dell'Economia Digitale tra Sviluppi Recenti
e Prospettive Future
a cura di Alessio Persiani

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.

ISSN (Online Edition): 2239 -7442