

Maria Cristina Gaeta

**LA PROTEZIONE DEI DATI
PERSONALI DELL'*INTERNET
OF THINGS*: L'ESEMPIO DEI
VEICOLI AUTONOMI**

Estratto



Milano • Giuffrè Editore

MARIA CRISTINA GAETA

LA PROTEZIONE DEI DATI PERSONALI NELL'INTERNET OF THINGS: L'ESEMPIO DEI VEICOLI AUTONOMI

SOMMARIO: 1. *Internet of things* e *Self-driving cars*: un'introduzione. — 2. L'interscambio dei dati personali nell'*Internet of things* con particolare riguardo ai *connected vehicles*. — 3. *Segue*. L'interrelazione possibile fra i processi di profilazione e di pseudonimizzazione. — 4. La scelta del metodo di indagine: analisi comportamentale e studi empirici. — 5. La necessità di una disciplina normativa per i veicoli autonomi. — 6. La (non) rilevanza del consenso al trattamento dei dati personali. — 7. La *Data protection by design* come particolare strumento per il rafforzamento della tutela preventiva dei dati personali.

1. INTERNET OF THINGS E SELF-DRIVING CARS: UN'INTRODUZIONE.

Al giorno d'oggi la pervasività della rete Internet¹ appare innegabile. Essa incide sulla vita privata e lavorativa di ogni essere umano che risulta costantemente monitorato attraverso la crescente quantità di tecnologie di identificazione e tracciamento.

¹ Con la rete Internet, infatti, si determina un'interconnessione globale tra reti informatiche di natura e di estensione diversa (LAN, WLAN, WAN, GAN e così via) i cui dispositivi dialogano tra loro mediante una suite di protocolli di comunicazione — TCP (*Transmission Control Protocol*) e IP (*Internet Protocol*) — consentendo il trasferimento da un utente all'altro di dati che possono essere pubblicati o condivisi. I dispositivi interconnessi o nodi ospitanti (c.d. *host*) seguono prevalentemente il modello *server-client* che consiste nell'insieme di un sottosistema informatico di elaborazione e gestione del traffico dati (*server*) che fornisce qualsiasi tipo di servizio ad altri componenti detti *clients*, consentendo loro di condividere le informazioni. Ne costituisce una

valida alternativa il modello *peer to peer* (P2P) in cui i ruoli del *server* e del *client* possono essere scambianti. Cfr. G. PASCUZZI, *Il diritto nell'era digitale*, 3^a ed., Bologna, 2016, pp. 23-24. Alla stregua del nostro ordinamento, l'art. 1, lett. *dd*, d.lgs. n. 259/2003 (Codice delle comunicazioni elettroniche) fornisce poi una esplicita definizione delle reti di comunicazione elettronica: « i sistemi di trasmissione e, se del caso, le apparecchiature di commutazione o di instradamento e altre risorse, inclusi gli elementi di rete non attivi, che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, comprese le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utiliz-

Tuttavia, i servizi offerti nel *web* risultano estremamente utili o, meglio, essenziali per la maggior parte delle attività quotidiane ².

La pervasività di Internet è stata notevolmente accentuata dalla sua estensione al mondo degli oggetti, realtà conosciuta come *Internet of things* (IoT). In particolare si tratta di un'evoluzione della rete Internet grazie alla quale gli oggetti interagiscono tra loro attraverso sensori e senza l'intervento umano, scambiandosi informazioni e accedendo ai contenuti presenti nelle banche dati ³. L'IoT è un'architettura dell'informazione che facilita lo scambio di beni e servizi e si traduce in un *network* informatico che collega tra loro oggetti — fisici o virtuali — che si rendono riconoscibili e acquisiscono intelligenza grazie alla possibilità di comunicare dati su se stessi e sull'ambiente che li circonda ⁴. Tali oggetti sono stati definiti, appunto, oggetti intelligenti (*smart things*) e sono contrassegnati da un *Radio Frequency Identifica-*

zate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui siano utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato ». In tal senso anche art. 2, co. 1, lett c, d.lgs. n. 177/2005 (Testo unico dei servizi di media e radiofonici).

² Quindi Internet e, più in generale, le nuove tecnologie rappresentano uno sviluppo delle libertà verso nuove frontiere dell'agire umano, reso possibile proprio a seguito del progresso tecnologico. In tal senso T.E. FROSINI, *Internet e democrazia*, in questa *Rivista*, IV-V, 2017, pp. 658 ss.. Nell'ambito di Internet, l'*Internet of Things* sta rivoluzionando la società contemporanea. Si tratta di una rivoluzione differente ma parallela a quella che vede come protagonista la robotica. Invero, anche lo sviluppo della robotica — e conseguentemente dell'intelligenza artificiale — risulta essere in grado di trasformare le abitudini di vita e lavorative di ciascuno di noi, di aumentare l'efficienza, il risparmio e la sicurezza, nonché di migliorare i servizi, apportando notevoli benefici non solo in ambito manifatturiero e commerciale, ma anche in diversi settori come, ad esempio, proprio quello dei trasporti (Risoluzione del Parlamento europeo recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica, 16.02.2017, 2015/2103(INL), cons. E, in *www.europarl.europa.eu*). In tal senso anche la Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, sulla revisione intermedia dell'attuazione della stra-

tegia per il mercato unico digitale, del 19.05.2017, COM(2017) 288, in *www.eur-lex.europa.eu*, pp.1 ss.; il ruolo della tecnologia nella trasformazione dell'Unione europea viene evidenziato anche nel Libro bianco sul futuro dell'Europa, Riflessioni e scenari per l'UE a 27 verso il 2025, 01.03.2017, COM(2017) 2025, in *www.eur-lex.europa.eu*, p. 4.

³ Con il termine banca dati (*database*) ci si riferisce alla raccolta di informazioni, organizzate in modo da consentirne all'utente un rapido reperimento. Tecnicamente la struttura del *database* è organizzata su tre livelli: 1) l'unità di memoria fisica che contiene il materiale, cioè l'elaboratore elettronico; 2) lo schema di disposizione del materiale inteso come il modello logico scelto dal programmatore (ad. esempio modello gerarchico, modello relazionale, ecc.); 3) il *software* per la consultazione delle informazioni memorizzate (*database management system*). Gli utenti interagiscono con la banca dati attraverso un terminale (dispositivo *hardware*), utilizzando un linguaggio di interrogazione (*query language*). A.M. GAMBINO, *Informatica giuridica e diritto dell'informatica*, in *Diritto online*, Treccani, 2013, p. 13.

⁴ *European Research Cluster on the Internet of Things (IERC), Internet of Things Strategic Research Roadmap*, in *www.internet-of-things-research.eu*, 2ª ed., 2011, p. 10: « [...] dynamic global network infrastructure with self configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes, and virtual personalities, use intelligent interface, and are seamlessly integrated into the information network ».

tion tag con un unico ID denominato *Electronic Product Code* (EPC) ⁵. Attualmente rientrano in questa categoria gli oggetti più disparati (semafori, automobili, termostati, frigoriferi, sveglie, orologi, telecamere di sorveglianza e molti altri) e sono così numerosi gli oggetti connessi che il concetto di “*Internet of things*” è stato in gran parte sostituito da quello di “*Internet of everything*”. Le interconnessioni, inoltre, sono in continua crescita e si prevede che entro il 2020 più di venti miliardi di oggetti saranno connessi tra loro ⁶.

In quest'ambito uno dei settori che segna il maggiore sviluppo è senza dubbio quello automobilistico con l'introduzione dei veicoli autonomi, cioè veicoli automatici in grado di soddisfare le principali funzioni di trasporto di un'autovettura tradizionale ⁷. Si prevede, infatti, che entro un ventennio circa 250 milioni di

⁵ Il *Radio Frequency Identification* (RFID) è una tecnologia basata su onde elettromagnetiche che comunica con delle etichette intelligenti (c.d. *tag*), capaci di leggere i numeri di identificazione univoca grazie ad un lettore (c.d. *reader*) e un sistema informatico in grado di identificare un determinato oggetto tramite il suo numero di identificazione, Pallone E. K., “*Internet of Things*” e l'importanza del diritto alla privacy tra opportunità e rischi, in *Cyberspazio e diritto*, vol. 17, n. 55, 2016, pp. 174 s.. Per un'ampia disamina sulla definizione di Internet delle cose cfr. R.H. WEBER, *Internet of Things, New security and privacy challenges*, in *Computer law & security report*, 2010, pp. 23 s.. Quanto all'introduzione del termine *Internet of Things*, risulta essere stato utilizzato per la prima volta da Kevin Ashton, cofondatore e direttore esecutivo di Auto-ID Center (consorzio di ricerca con sede presso il Massachusetts Institute of Technology), durante una presentazione presso *Procter & Gamble* nel 1999, come espressamente dichiarato dall'autore e confermato dalla dottrina maggioritaria (Cfr. ASHTON K., *That “Internet of Things” Thing. In the real world, things matter more than ideas*, in *RFID Journal*, 2009, p. 1). Tuttavia quella che può essere definita come la nascita dell'IoT è stimata agli inizi del XXI secolo, quando il numero di dispositivi connessi in rete ha superato quello della popolazione mondiale (Cfr. S. HALLER, S. KARNOUSKOS, C. SCHIROH, *The Internet of Things in an enterprise context*, conference paper, in *Future Internet, Lecture Notes in Computer Science*, vol. 5468, 2008, p. 1).

⁶ Studio Gartner, *Leading the IoT*, *Gartner insight on how to lead in a connected world*, in www.gartner.com, 2017, p. 13.

Inoltre, il McKinsey&Company ha evidenziato che entro il 2030 vi sarà un forte sviluppo dell'attuale realtà sociale che sarà fondato su tre modelli di mobilità urbana avanzata (*clean and shared mobility, private autonomy, and seamless mobility*), applicabili in maniera diversa a seconda della città di riferimento, in quanto i contesti locali sono i più disparati. Infatti, in ogni città vi sono diversi livelli di traffico stradale e, conseguentemente, diversi livelli di inquinamento ambientale, differenti condizioni atmosferiche, particolari connotazioni dei luoghi e, infine, la forza degli organi esecutivi locali varia di territorio in territorio. In termini generali, la mobilità — con particolare riguardo all'autonomia e all'elettrificazione — sarà combinata con i sistemi integrati di energia, con i trasporti pubblici e con le infrastrutture. Notevoli saranno anche i vantaggi in termini di *business*. Per un maggiore approfondimento si veda E. HANNON, C. McKERRACHER, I. ORLANDI e S. RAMKUMAR, *An integrated perspective on the future of mobility*, in www.mckinsey.it, 2016, pp. 1 ss.

⁷ Lo sviluppo delle *self-driving cars* ha avuto inizio circa trent'anni orsono con il progetto PROMETHEUS (*PROgramMme for European Traffic with Highest Efficiency and Unprecedented Safety*), lanciato nel 1987 da Mercedes-Benz. Risultato del progetto sono stati i due veicoli gemelli VaMP e VITA-2 che percorsero più di 1.000 chilometri di traffico in modalità completamente autonoma sulle autostrade di Parigi nel 1994. Nel 2004, poi, la *Defence Advanced Research Project Agency* (DARPA) organizzò il primo *Grand Challenge*, gara in cui i veicoli autonomi dovevano attraversare il Deserto del Mojave (California). Sfortunatamente nessuno dei partecipanti alla gara terminò il

autoveicoli saranno connessi in rete ⁸ e il mercato automobilistico — fondato in larga misura sul *cloud computing* — crescerà esponenzialmente, fino a quadruplicarsi ⁹. Per di più, intorno al 2025 si raggiungerà un livello di automazione tale (livello 3 dello standard SAE J3016) ¹⁰ che il conducente non avrà l'obbligo di monitorare costantemente il veicolo, anche se dovrà essere in grado di riprenderne il controllo in ogni momento.

Naturalmente i veicoli autonomi, per comunicare tra loro,

percorso (142 miglia) e i veicoli che si spinsero più lontano percorsero meno di 8 miglia. Nel *Second Grand Challenge* che si tenne l'anno successivo, invece, cinque veicoli completarono con successo il percorso di 132 miglia nel Nevada e a vincere fu il *team* di Sebastian Thrun dell'Università di Stanford (uno degli inventori di *Google Street View* che dal 2009 lavora al progetto iniziato come *Google self-driving car* e attualmente denominato *Waymo (New way forward in mobility)*). Successivamente, nella *Third Grand Challenge* (2007) sei veicoli completarono la gara. Un altro esperimento in tal senso è stato realizzato nel 2010 in Italia dove, grazie al progetto *Vislab* dell'Università di Parma — diretto dal Professor Alberto Broggi — furono inviati con successo due furgoni senza conducente lungo un percorso di più di 15.000 km, da Roma a Shanghai. Successivamente, nel 2013 il Prof. Broggi ha messo in circolazione sulle strade di Parma il veicolo senza guidatore BRAiVE in un percorso misto extraurbano e urbano (*Public ROad Urban Driverless-Car Test* 2013). Infine, di recente si sono inseriti nel mercato dei veicoli autonomi anche l'azienda automobilistica Tesla, che nel 2016 ha già messo in commercio il modello S e il modello X, e Uber, l'azienda di trasporto automobilistico che nello stesso anno ha iniziato ad utilizzare le *driverless cars* per il servizio di trasporto passeggeri e nel 2017 anche la Ford ha iniziato ad investire nel settore dell'intelligenza artificiale per i suoi futuri veicoli a guida autonoma con l'acquisizione di Argo AI, startup fondata da ex dirigenti di Google e Uber e specializzata proprio in sistemi di intelligenza artificiale. (Fonti: Eureka, *Programme for a european traffic system with highest efficiency and unprecedented safety*, in www.eurekanetwork.org; *The DARPA Grand Challenge: Ten Years Later*, in www.darpa.mil, 2014; www.waymo.com; *La sfida del VisLab conclusa con successo: i veicoli automatici hanno raggiunto l'Expo di Shanghai*, in www.vislab.it, 2010; *Nuovo esperimento su strada della tecnologia VisLab: guida in città*, in www.vislab.it, 2013; Tesla, *Guida autonoma disponibile su tutte le auto*, [\[sla.com\]\(http://sla.com\); *Self-Driving Ubers, the world's first Self-Driving Ubers are on the road in the Steel City*, in \[www.uber.com\]\(http://www.uber.com\); Ford, la "parola" ai veicoli autonomi, in \[www.lautomobile.aci.it\]\(http://www.lautomobile.aci.it\), 2017\).](http://www.te-</p>
</div>
<div data-bbox=)

⁸ Stime Gartner, *Gartner Says By 2020, a Quarter Billion Connected Vehicles Will Enable New In-Vehicle Services and Automated Driving Capabilities*, in www.gartner.com, 2015; secondo MCKINSEY, *Disruptive technologies: Advances that will transform life, business, and the global economy*, in www.mckinsey.com, 2013, l'impatto economico dell'automazione dovrebbe raggiungere valori compresi tra 6.500 e 12.000 miliardi di euro entro il 2025.

⁹ Stime Price Waterhouse Cooper, *In the fast lane, the bright future of connected cars*, in www.strategyand.pwc.com, 2014, p. 5.

¹⁰ I livelli di automazione sono stati classificati da molteplici autori. Un'interessante classificazione, ampiamente condivisa, prevede cinque *vehicle automation degrees* che vanno dal completo controllo del veicolo da parte del conducente al completo controllo direttamente operato dal veicolo stesso: *driver only*, *driver assistance*, *partial automation*, *high automation* e *full automation*; tale classificazione, peraltro, è in linea con quanto ammesso dalla *National Highway Traffic Safety Administration* (NHTSA), che ha anch'essa previsto cinque livelli in materia di automazione: *no-automation*, *function-specific automation*, *combined function automation*, *limited self-driving automation* e *full self-driving automation*. Si veda T.M. CASSER e D. WESTHOFF, *Definitions of Automation and Legal Issues in Germany, workshop of German Federal Highway Research Institute*, in www.ssrn.com, 2012; *Human Factors Evaluation of Level 2 And Level 3 Automated Driving Concepts*, U.S. Department of Transportation of National Highway Traffic Safety Administration, in www.nhtsa.gov, 2014, 2 s.. Nel 2014 la SAE International ha pubblicato un nuovo standard internazionale J3016 che ha definito sei differenti livelli per la guida autonoma: *driver only*, *assisted*, *partial automation*, *conditional automa-*

devono essere connessi in rete ed è da questa circostanza che scaturisce l'inclusione anche del settore automobilistico nel *network* dell'*Internet of Things*. Le tipologie di connessione che vedono come protagonisti i veicoli automatizzati — i quali vengono spesso definiti come *connected vehicles* proprio per enfatizzare la loro capacità di connettersi in rete — sono sostanzialmente tre. La prima e più comune forma di comunicazione è quella che intercorre tra i veicoli automatizzati e le più svariate categorie di dispositivi — tra i più comuni vi sono gli *smartphone*, gli *smart watch*, i *tablet* e i *personal computer*, i quali possono essere connessi ai veicoli di ultima generazione tramite apposite applicazioni installate su tali dispositivi — nota come la *Vehicle to device communications* (V2D). Altra forma di comunicazione è la *Vehicle to infrastructure communications* (V2I), una tipologia più specifica che si instaura tra i veicoli e le infrastrutture (ad esempio, i semafori stradali o gli strumenti di controllo della velocità, quali i tutor oppure gli autovelox). Infine, la più sofisticata tipologia di comunicazione è quella *Vehicle to vehicle communications* (V2V), la quale presuppone che siano messi in circolazione veicoli completamente autonomi o, quantomeno, dotati di un elevato livello di automazione¹¹. Premesso che per predisporre tali forme di connessione è necessario che i veicoli siano — anche solo parzialmente — automatizzati, appare evidente come il grado di comunicazione dei veicoli sia direttamente proporzionale al relativo livello di automazione degli stessi, anche se il sistema di connessione è solo uno dei presupposti necessari per raggiungere la completa automazione del veicolo.

Grazie allo sviluppo della guida autonoma e conseguentemente connessa, la mobilità è destinata a evolversi sempre più rapidamente comportando notevoli benefici, tra i quali il miglioramento delle condizioni del traffico stradale, la riduzione dell'inquinamento ambientale, lo sviluppo della *sharing economy*, la maggiore sicurezza dei trasporti e l'estensione della mobilità anche a favore di soggetti ai quali la guida è di regola preclusa — bambini, anziani e disabili — trasformando la mobilità in un vero e proprio servizio (*mobility as a service*)¹². L'IoT è senza dubbio la più importante innovazione della *Information Technology* (IT), tut-

tion, high automation e full automation. Cfr. SAE standard J3016, *Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems*, in www.sea.org, 2014 (rivisto nel 2016 ma i livelli di automazione sono gli stessi). Sui veicoli connessi e autonomi è stato condotto uno studio nel Regno Unito, il quale ha ripreso i sei livelli di automazione dello standard SAE evidenziando che entro il 2030 il 25% dei veicoli in UK sarà completamente

autonomo, v. KPMG Study, *Connected and Autonomous Vehicles. The UK Economic Opportunity*, in www.kpmg.co.uk, 2015, p. 9.

¹¹ Par. II, lett. d., *Declaration of Amsterdam, Cooperation in the field of connected and automated driving*, 14-15.04.2016, in www.regjeringen.no.

¹² In tal senso l'Introduzione della *Declaration of Amsterdam*, cit..

tavia, oltre ai molteplici vantaggi, si rilevano numerose questioni ancora aperte e il settore automobilistico — in cui l'IoT trova senz'altro applicazione — risulta essere quello in cui è avvertita con maggiore urgenza la necessità di una regolamentazione¹³. Una delle principali problematiche da affrontare è quella concernente i nuovi profili di responsabilità configurabili in caso di incidenti stradali causati dal malfunzionamento della *driverless car*. La questione è già stata approfondita in altri contributi ai quali si rinvia¹⁴. Nel presente lavoro — alla luce della riforma europea sulla *data protection*¹⁵ — appare opportuno soffermarsi sulle questioni inerenti la tutela dei dati personali trasmessi dai veicoli autonomi e la relativa profilazione dell'utente che utilizza quotidianamente tali tecnologie, spesso ignaro delle relative conseguenze non sempre ottimali¹⁶.

2. L'INTERSCAMBIO DEI DATI PERSONALI NELL'INTERNET OF THINGS CON PARTICOLARE RIGUARDO AI CONNECTED VEHICLES.

La tutela dei dati personali¹⁷ è da sempre una questione che riveste grande rilevanza sociale, riproponendosi di epoca in epoca

¹³ Risoluzione del Parlamento europeo, cit., punti nn. 24 ss.

¹⁴ A. DAVOLA e R. PARDOLESI, *In viaggio col robot: verso nuovi orizzonti della r.c. auto ("driverless")?*, in *Danno e resp.*, 2017, V, pp. 616 ss.. Mi sia consentito rinviare anche a M.C. GAETA, *Automazione e responsabilità civile automobilistica*, in *Resp. civ. e prev.*, 2016, V, pp. 1718 ss..

¹⁵ Il 4 maggio 2016 sono stati pubblicati sulla Gazzetta Ufficiale dell'Unione Europea (GUUE) i testi normativi che costituiscono il c.d. pacchetto protezione dati: il Regolamento del Parlamento europeo e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE, 27.04.2016, n. 679 (d'ora in poi permettete che si utilizzi l'acronimo inglese GDPR); la Direttiva del Parlamento europeo e del Consiglio relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio, 27.04.2016, n. 680; la Direttiva del Parlamento europeo e del Consiglio sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi,

27.04.2016, n. 681, in *www.eur-lex.europa.eu*.

¹⁶ G. ALPA, prefazione, R. PARDOLESI (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003, pp. VII ss. sulla protezione dei dati personali afferma che: «È pure una disciplina difficile da articolare e tradurre in normative, sia per il bilanciamento di interessi che implica, sia per la volatilità delle previsioni, destinate a consumarsi nel corso della evoluzione delle tecnologie e dell'affinamento della coscienza sociale e quindi della "reattività" dei singoli alle iniziative e ai fenomeni che possono porre in pericolo la loro riservatezza.». S. RODOTÀ, *Tecnologie dell'informazione e frontiere del sistema socio-politico*, in *Pol. dir.*, 1982, pp.25 ss. ritiene che le regole giuridiche si devono adattare al ritmo veloce del cambiamento tecnologico.

¹⁷ Il termine "dato personale" fa riferimento a tutte le informazioni relative a una persona fisica identificata o identificabile (art. 4, par. 1, lett. a, Reg. 2016/679/UE e art. 4, co. 1, lett. b, D.lgs. 30.06.2003, n. 196) ed è considerato un bene giuridico immateriale, rientrante nel novero dell'art. 810 c.c.. Nello specifico, le informazioni relative all'utente o agli utenti di bordo del veicolo diventano dati personali nei casi in cui gli stessi siano soggetti identificati o, comunque, identificabili. V. ZENO-ZENCOVICH, *Una lettura comparatistica della L. 675/96 sul trattamento dei*

sotto differenti aspetti. Nel linguaggio corrente i termini riservatezza, *privacy* e protezione dei dati personali sono spesso utilizzati come sinonimi anche se si tratta di fattispecie in parte diverse, seppur tra loro correlate. Il diritto alla riservatezza può, infatti, essere suddiviso in due accezioni: una, più tradizionale, consiste nel diritto alla non divulgazione dei fatti della vita privata; un'altra, più innovativa, che fa riferimento alla tutela dell'intimità della sfera privata (c.d. *privacy*)¹⁸. La tradizionale accezione di diritto alla riservatezza è ormai confluita nel diritto alla protezione dei dati personali, libertà fondamentale¹⁹ e autonomo diritto della personalità²⁰ che si manifesta nel potere di autodefinirsi. Il diritto alla riservatezza si può dunque suddividere in diritto alla *privacy* e diritto alla protezione dei dati personali²¹; tale distinzione trova un evidente riscontro nella Carta di Nizza, agli artt. 7 e 8 che disciplinano rispettivamente le due distinte fattispecie²². Tuttavia, il diritto alla tutela dei dati personali — pur costituendo un autonomo diritto della personalità — è una specificazione del diritto alla *privacy*, dato che uno dei casi

dati personali, in V. CUFFARO, V. RICCIUTO e V. ZENO-ZENCOVICH (a cura di), *Trattamento dei dati e tutela della persona*, Milano, 1998, pp. 167 ss. classifica i dati personali come beni giuridici in quanto sono suscettibili di formare oggetto di diritti; in particolare, sono cedibili, trasferibili, scambiabili e, di regola, danno vita a rapporti obbligatori e negoziali. Ciò non comporta una violazione del principio dell'indisponibilità dei diritti della personalità (considerato dallo stesso autore come principio di incerto fondamento) dato che conferendo il consenso al trattamento dei dati personali non si rinuncia alla personalità.

¹⁸ Il diritto alla *privacy* è stato introdotto dalla dottrina americana nel XIX secolo quale “*right to be let alone*”, nel senso di non subire ingerenze nelle proprie questioni personali. Il termine fu coniato da Samuel D. Warren e Louis Brandeis, autori del saggio intitolato *Right to privacy*, pubblicato nel 1980 nella *Harvard Law Review*. Per una chiara e concisa rievocazione della vicenda T. E. FROSINI, *Liberté, Egalité, Internet*, Napoli, 2015, pp. 139-140.

¹⁹ T. E. FROSINI, *Liberté ecc.*, cit., p. 142, è categorico nell'affermare che per il diritto alla *privacy* non sono ammesse situazioni di incertezza: « o è un diritto fondamentale oppure no ». Ciò nonostante, essendo un diritto fondamentale — e la collettività vuole che lo sia — occorre tutelarlo come tale. G. F. AIELLO, *La protezione dei dati personali dopo il Trattato di Lisbona. Natura e limiti di un diritto fondamentale*

« *disomogeneo* » alla luce della nuova proposta di General Data Protection Regulation, in *Osservatorio del diritto civile e commerciale*, II, 2015, pp. 16 ss., il quale definisce il diritto alla protezione dei dati personali come disomogeneo diritto fondamentale in virtù della nozione tanto ampia di dato personale, nella quale rientrano le categorie più disparate di dati compresa (ma non solo) quella inerente la dignità umana, che sarebbe configurabile come diritto inviolabile e non « meramente » fondamentale, ai sensi del art. 1, Carta dei diritti fondamentali dell'Unione europea, 18.12.2000, C 364/3, in www.europarl.europa.eu (c.d. Carta di Nizza).

²⁰ P. RESCIGNO, *Protezione dei dati e diritti della personalità*, in V. CUFFARO, V. RICCIUTO, V. ZENO-ZENCOVICH (a cura di), *Trattamento dei dati e tutela della persona*, Milano, 1998, p. 277 ss., enfatizzava i diritti della personalità come fondamento positivo per la tutela del diritto alla riservatezza già all'epoca della l. n. 675/1996.

²¹ Nell'art. 2 del Codice in materia di protezione dei dati personali, al primo comma, è evidente la distinzione tra riservatezza (da intendersi nell'accezione di *privacy*), identità personale e diritto alla protezione dei dati personali. Cfr. D.lgs. 30.06.2003, n. 196, in www.normattiva.it (c.d. codice *privacy*).

²² C.M. BIANCA e F.D. BUSNELLI, (a cura di), *La protezione dei dati personali*, tomo I, Padova, 2007, pp. XX ss.; C.M. BIANCA, *Diritto civile*, vol. I, *La norma giuridica. I soggetti*, 2ª ed., Milano, 2002, p. 180.

in cui viene leso il diritto al rispetto della *privacy* è quello dell'abusivo trattamento dei dati personali.

In questa sede si tenterà di analizzare il diritto alla protezione dei dati personali interscambiati nell'IoT, con particolare riguardo ai veicoli autonomi e connessi.

L'impatto trasversale che la rete Internet — e ancor di più l'IoT — ha avuto nella realtà contemporanea, ha attirato l'attenzione delle Autorità Pubbliche sia a livello nazionale che europeo. Segnatamente, il Gruppo di lavoro ex articolo 29 per la protezione dei dati personali²³ ha adottato nel 2014 un parere diretto a trovare soluzioni tali da rendere applicabile la normativa della tutela dei dati personali anche nell'ambito dell'Internet delle cose²⁴. Sulla base di un approccio tipico dell'analisi economica del diritto, il *Working group* 29 ha messo a confronto gli interessi dei cittadini alla tutela dei propri dati personali e quelli delle aziende che operano nel settore — le quali traggono notevoli benefici economici dalla diffusione dell'IoT — tentando di dettare delle linee guida per rendere applicabile l'esistente normativa europea in materia anche ai dati personali scambiati nell'ambito dell'Internet degli oggetti.

L'anno seguente il Garante italiano per la protezione dei dati personali ha deciso di avviare una consultazione pubblica sul tema, al fine di definire il fenomeno e introdurre nuove regole atte ad assicurare agli utenti la tutela dei dati personali e la massima trasparenza nel loro utilizzo²⁵. Per lo stesso motivo il *Global Privacy Enforcement Network* (GPEN)²⁶ ha avviato il *Privacy Sweep* 2016 — un'indagine a carattere internazionale atta a verificare il rispetto della sfera privata e dei dati personali nell'IoT — rafforzando la cooperazione tra le Autorità per la

²³ Istituito ex art. 29, Dir. 95/46/CE, è un organismo consultivo e indipendente per la protezione dei dati personali, composto da un rappresentante dell'autorità preposta alla protezione dei dati personali designata da ciascuno Stato membro, dal Garante europeo della protezione dei dati e da un rappresentante della Commissione.

²⁴ Parere del Gruppo di lavoro per la protezione dei dati personali, sui recenti sviluppi nel campo dell'Internet degli oggetti, 16.09.2014, n. 3, in *www.ec.europa.eu*, pp. 10 ss., il quale fa esplicito riferimento a *Wearable Computing, Quantified Self e domotics*, ma appare applicabile in via analogica a qualsiasi ambito dell'IoT.

²⁵ Decisione del Garante per la protezione dei dati personali, 26.03.2015, n. 179, in *www.garanteprivacy.it*; Comunicato stampa del Garante per la protezione dei dati personali, "Internet delle cose": il Garante privacy avvia consultazione per defi-

nire le regole e tutele, in *www.garanteprivacy.it*, 28.04.2015.

²⁶ Nel 2007, il Consiglio dell'*Organisation for Economic Cooperation and Development* (OECD) ha adottato la *Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy*. La raccomandazione aveva imposto ai Paesi membri dell'OECD l'obiettivo di creare un *informal network* di Autorità per la protezione dei dati personali, da cui è nato il *Global Privacy Enforcement Network*. Le Autorità garanti del GPEN devono cooperare nell'applicazione della legge sulla *privacy*, condividere le migliori strategie per affrontare le sfide transfrontaliere, lavorare congiuntamente per lo sviluppo di iniziative comuni e di campagne di sensibilizzazione. Tale cooperazione deve avvenire nel rispetto delle disposizioni della raccomandazione e dei relativi ordinamenti giuridici.

tutela dei dati personali dei ventisei Paesi del mondo che hanno aderito all'iniziativa ²⁷. L'indagine si è conclusa il 22 settembre 2016 con risultati preoccupanti. Infatti, più del 60% degli oggetti intelligenti connessi in rete non ha superato l'esame del GPEN ²⁸.

Quanto ai veicoli autonomi, appare evidente che dall'interconnessione degli stessi derivi la raccolta, l'elaborazione e il trasferimento di dati, che spesso sono dati personali o, addirittura dati sensibili ²⁹. Tale tipologia di trattamento dei dati personali, focalizzato sui veicoli autonomi ovvero sulla mobilità più in generale, è attualmente oggetto di approfondita indagine ³⁰. Estremamente recente è la ricerca commissionata dalla Federazione Internazionale dell'Automobile (FIA) — avente ad oggetto il flusso dei dati scambiati tra le vetture e le rispettive aziende produttrici — la quale ha rivelato la quantità e la qualità di dati che i veicoli di ultima generazione sono in grado di scambiare in rete ³¹. Per di più, sulla base dei risultati di questa ricerca, la FIA ha lanciato il

²⁷ Il *Privacy Sweep 2016* analizza il funzionamento di dispositivi molto diversi fra loro: orologi che misurano il battito cardiaco e la pressione sanguigna, frigoriferi che segnalano la scadenza dei cibi riposti al loro interno, contatori che regolano automaticamente la temperatura, veicoli completamente autonomi che portano il conducente (o meglio il passeggero) direttamente a destinazione e così via. Cfr. Comunicato stampa del Garante per la protezione dei dati personali, *"Internet delle cose" sotto la lente delle Autorità garanti privacy*, in www.garanteprivacy.it, 11.04.2016.

²⁸ Precisamente, il 59% delle *smart things* non offre adeguate informazioni su come siano raccolti, utilizzati e comunicati a terzi i dati personali degli utenti, il 68% non fornisce adeguate informazioni sulle modalità di conservazione dei dati stessi, il 72% non spiega agli utenti come cancellare i dati dal dispositivo e il 38% non garantisce agli utenti semplici chiarimenti in merito al rispetto della propria *privacy*. Migliori, invece, sono stati i risultati delle analisi condotte dal Garante italiano sul rispetto dei dati personali da parte di alcune delle principali aziende produttrici nel settore della domotica. Specificamente è stato riscontrato che solo il 10% non fornisce agli utenti alcuna informazione su come i loro dati personali siano raccolti, utilizzati e comunicati a terzi. Per un maggiore approfondimento v. Comunicato stampa del Garante per la protezione dei dati personali, *Privacy: "Internet delle cose", utenti poco tutelati. I risultati dell'analisi internazionale*

svolta dalle Autorità garanti della privacy di 26 Paesi per il "Privacy Sweep 2016", in www.garanteprivacy.it, 22.09.2016.

²⁹ A. WOOD, D.R. O'BRIEN e U. GASSER, *Privacy and Open Data*, in *Networked Policy Series*, in cyber.harvard.edu, 2016, p. 4.

³⁰ A titolo esemplificativo si segnalano: Garante per la protezione dei dati personali, www.garanteprivacy.it, Federazione Internazionale dell'Automobile, www.fia.com; PricewaterhouseCooper, www.pwc.com; KPMG, www.kpmg.com.

³¹ La ricerca si è composta di un sondaggio basato su dodicimila questionari compilati in dodici Paesi (tra cui l'Italia) e di uno studio tecnico condotto dall'ADAC (*Automobil club* tedesco), la quale ha preso in considerazione due veicoli, uno ad alimentazione tradizionale e l'altro ad alimentazione elettrica, dimostrando che tali veicoli registrano e possono trasmettere i dati personali dei passeggeri, oltre a tracciare una profilazione degli stessi. Precisamente è stato dimostrato che l'automobile tradizionale ha memorizzato dati riguardanti le diverse modalità di guida da parte del conducente, la tensione delle cinture di sicurezza a seguito di frenata improvvisa, il numero dei viaggi e i chilometri percorsi, le ultime destinazioni inserite nel sistema GPS, i giri del motore, il chilometraggio del veicolo, lo stato delle luci e i dati generati dalla sincronizzazione con il telefonino (che a loro volta implicano altre informazioni come il numero dei passeggeri, il sesso, l'età, le abitudini, ecc.). Nell'automobile elettrica, invece, l'ADAC ha identi-

progetto *My Car My Data* ³², atto ad incrementare la consapevolezza degli utenti circa i dati personali trattati e ad evidenziare la necessità di introdurre una normativa specifica.

Dai risultati del progetto *My Car My Data*, si evince che la fonte dei dati derivanti dalla connessione dei veicoli può essere sia l'utente (*customer provided data*) che il veicolo autonomo (*vehicle generated data*) ³³. Nel primo caso, i dati sono senza dubbio dati personali del proprietario del veicolo, del conducente del veicolo ovvero di eventuali passeggeri a bordo dello stesso. Essi riguardano, ad esempio, la localizzazione dell'autoveicolo e dei suoi passeggeri, i tragitti percorsi e le informazioni derivanti dalla sincronizzazione del cellulare degli utenti a bordo con l'auto connessa. Nel secondo caso, invece, i dati sono prodotti dal veicolo stesso e possono essere dati personali o semplici dati tecnici (*technical data*). Secondo l'orientamento maggioritario ³⁴ — che ha carattere restrittivo — rientrano nella categoria di *technical data* solo quei dati che non possono essere in nessun modo ricollegati all'utente, altrimenti si tratta di dati personali o sensibili. Ad esempio, il dato tecnico relativo al livello dell'olio nel motore del veicolo diventa un dato personale se è collegabile con un utente specifico, in quanto consente di porre in essere deduzioni riguardanti la sua sfera personale.

L'interessato del trattamento — che deve fornire il consenso per il trattamento dei suoi dati personali — può essere il proprietario del veicolo, il conducente ovvero un passeggero. La questione della titolarità dei dati (intesa come *ownership*) è intuitiva nel caso in cui si tratti di *customer provided data* che, appunto, sono riconducibili ai soggetti appena elencati e, in quanto dati perso-

ficato, tra l'altro, i luoghi e le modalità di ricarica, le coordinate delle ultime cento soste, se e dove il conducente ha preso un altro mezzo di trasporto, nonché la qualità della batteria e il tipo di connettore utilizzato. I risultati dimostrano che il 90% degli utenti ritiene che i dati siano di sua proprietà, il 91% vuole poter attivare e disattivare la connessione del veicolo, il 76% vuole poter decidere quando condividere i propri dati personali e il relativo lasso temporale della condivisione e — astrattamente di estrema rilevanza — il 95% degli utenti richiede una legislazione che protegga i dati personali collegati ai *connected vehicles* dichiarando di essere preoccupati per la divulgazione degli stessi. Cfr. *FIA reveals what data is being tracked and how the public reacts to connected cars*, in www.fia.com, 2015.

³² Si tratta di una campagna interna-

zionale di sensibilizzazione degli utenti sulla tutela dei dati personali in relazione ai veicoli autonomi. Per un ampio approfondimento www.mycarmydata.com.

³³ Fédération internationale de l'automobile (FIA), *What EU legislation says about car data*, Legal Memorandum on connected vehicle and data, in www.osborneclarke.com, 2017, pp. 1 ss.

³⁴ Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Una strategia europea per i sistemi di trasporto intelligenti cooperativi, prima tappa verso una mobilità cooperativa, connessa e automatizzata*, COM(2016) 766 final, 30.11.2016, p. 8. In tal senso anche la Corte di giustizia dell'Unione europea, sentenza del 19 ottobre 2016, Patrick Breyer/Bundesrepublik Deutschland, C-582/2014, EU:C:2016:779, punto 32.

nali, rientrano nell'ambito di applicazione del GDPR³⁵. Al contrario, quando si tratta di *vehicle generated data*, se i dati sono personali, è abbastanza agevole il collegamento con il soggetto che risulta essere l'interessato del trattamento e, in quanto tale, il titolare dei dati, risultando applicabile il GDPR. Quando, invece, i *vehicle generated data* non sono dati personali ma meri dati tecnici, non appare assolutamente facile individuarne il titolare né la normativa applicabile. Secondo autorevole dottrina, sembrerebbe opportuno individuare il titolare dei dati in colui che ha un maggiore interesse negli stessi³⁶. A proposito della normativa applicabile, poi, trattandosi di dati che esulano dall'applicazione del GDPR (in quanto non sono dati personali), si potrebbe ipotizzare l'introduzione di una normativa *ad hoc* per i dati generati dall'IoT che sono caratterizzati dal requisito della *novelty* e, quindi, sono nuovi dati. In tale categoria di nuovi dati, rientrerebbero quelli generati dalla connessione dei veicoli autonomi. Tuttavia non è semplice introdurre una normativa così specifica a causa delle molteplici incognite che riguardano tanto la materia da disciplinare quanto la titolarità di tali dati.

Quanto al titolare del trattamento, appare preferibile la tesi secondo cui siano configurabili, quali titolari del trattamento, il produttore del veicolo, il produttore di una componente elettronica del veicolo — compresa la scatola nera o il servizio *eCall* (v. *infra* par.VI) — ovvero soggetti terzi, quali ad esempio fornitori di un servizio³⁷. Tali soggetti raccolgono dati non solo sulla *performance* dei propri prodotti o sull'andamento del mercato ma anche dati personali degli utenti, che ne sono spesso inconsapevoli³⁸.

Appare opportuno, pertanto, domandarsi se attualmente l'informativa sul trattamento dei dati personali sia adeguata e se il relativo consenso sia valido³⁹. Il consenso⁴⁰ è la base giuridica o

³⁵ S. VAN ERP, *Ownership of data: the numerus clausus of legal objects*, in *Brigham-Kanner Prop. Rts. Conf. J.*, Vol. 6, 2017, pp. 9.

³⁶ T.J. FARKAS, *Data created by the Internet of Things: the new gold without ownership*, in *Rev. Prop. Immaterial*, vol. 23, 2017, pp. 7-8, fa riferimento all'interesse delle aziende automobilistiche a ricevere informazioni sui propri veicoli autonomi in commercio, a quello dei fornitori di servizi a ottenere *feedback* per migliorare i servizi offerti, a quello degli assicuratori che intendono raccogliere dati sulle dinamiche degli incidenti ovvero a quello del governo che ha bisogno di continui aggiornamenti relativi al traffico stradale.

³⁷ Fédération internationale de l'automobile (FIA), *op. cit.*, pp. 9 ss.

³⁸ A proposito dell'inconsapevolezza dell'utente si veda W.K. HON, C. MILLARD e J. SINGH, *Twenty Legal Considerations for Clouds of Things*, *Queen Mary University of London, School of Law, Legal Studies Research paper* no. 216/2016, in www.papers.ssrn.com, 2016, p. 23; A. MONTELEIRO, *Data protection, e-ticketing, and intelligent systems for public transport*, in *International Data Privacy Law*, vol. 5, n. 4, 2015, pp. 309 ss..

³⁹ In tal senso E.K. PALLONE, *op. cit.*, p. 177.

⁴⁰ Il consenso è definito nell'art. 4, par. 1, n. 11, Reg. 2016/679/UE come: « [...]

la condizione di liceità⁴¹ per il trattamento dei dati personali al quale si affiancano altri limiti, come i principi di finalità, necessità e proporzionalità, le misure di sicurezza per garantire la non dispersione dei dati e l'utilizzo conforme a quanto autorizzato dall'interessato o consentito dalla legge, il controllo delle autorità indipendenti e, infine, le sanzioni civili, penali e amministrative. La *ratio* del consenso è quella di garantire il potere di autodeterminazione del singolo circa l'accesso ai propri dati personali da parte di terzi e, contemporaneamente, il potere di controllo dello stesso soggetto sui suoi dati. Precisamente, in merito ai dati personali il consenso è condizione di liceità del trattamento (art. 7, GDPR) invece, quanto ai dati sensibili⁴², esso costituisce una deroga al divieto di trattamento, che altrimenti non sarebbe consentito (art. 9, GDPR)⁴³.

Una questione che merita di essere approfondita attiene ai rapporti tra il sempre più rapido sviluppo della tecnologia e la concreta possibilità di prestare un consenso razionale e consapevole. In tali casi, dunque, vi è un effettivo potere di autodeterminazione dell'utente? Il consenso viene realmente prestato in conformità alla normativa vigente? Il consenso risulta essere ancora uno strumento normativo adeguato e al passo con i tempi per la tutela della propria sfera personale?⁴⁴

qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento ».

⁴¹ A seconda se si preferisca la terminologia del nuovo Regolamento europeo in materia ovvero quella della Carta di Nizza. Conformemente I.A. CAGGIANO, *Il consenso al trattamento dei dati personali tra Nuovo Regolamento Europeo e analisi comportamentale*, in corso di pubblicazione, pp. 5 e 10.

⁴² I dati sensibili sono una categoria speciale di dati personali i quali, ai sensi dell'art. 9, Reg. 2016/679/UE, sono: « [...] l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché [...] dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona ». In tal senso anche art. 4, par. 1, lett. d., cod. *privacy*.

⁴³ I.A. CAGGIANO, *Il consenso al trattamento dei dati personali*, cit., pp. 10 ss.. Inoltre, l'autrice precisa che, con il GDPR, per il trattamento dei dati sensibili non è più richiesto alcun requisito di forma *ad substantiam* né l'autorizzazione del Garante per la protezione dei dati personali, che invece sono attualmente previsti dal legislatore nazionale (art. 26 cod. *privacy*).

⁴⁴ *Ivi*, pp. 5 s.. Inoltre, W.K. HON, C. MILLARD e J. SINGH, *op. cit.*, pp. 21 ss., sostengono che nella pratica sia difficile ottenere il requisito del consenso, specialmente di un consenso che sia libero, specifico, informato e inequivocabile in conformità con il GDPR. Più in generale, sulla *data protection*, G. FINOCCHIARO, *La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Schrems*, in G. RESTA e V. ZENO-ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali. Dai "safe harbour principles" al "privacy shield"*, Roma, 2016, p. 134, non considera per nulla soddisfacente l'attuale regolamentazione della protezione dei dati personali che, secondo la sua opinione (pienamente condivisibile), necessiterebbe di una riforma ben più ampia di quella contenuta nel GDPR.

3. *SEGUE*. L'INTERRELAZIONE POSSIBILE FRA I PROCESSI DI PROFILAZIONE E DI PSEUDONIMIZZAZIONE.

Il consenso dell'utente assume una particolare funzione in relazione alla profilazione. Con tale termine si fa riferimento a qualsiasi forma di trattamento automatizzato di differenti tipologie di dati personali afferenti a un elevatissimo numero di soggetti mediante specifici algoritmi, al fine di attribuire a ciascuno di essi un profilo. Più dettagliatamente, lo scopo della profilazione è quello di valutare determinati aspetti personali relativi a una persona fisica, come il rendimento professionale, la situazione economica, la salute, le preferenze, gli interessi, l'affidabilità, il comportamento, la localizzazione o gli spostamenti⁴⁵. Si crea così un profilo digitale dell'utente che costituisce un'ulteriore forma di rappresentazione dell'individuo rispetto all'identità personale⁴⁶ — cioè quell'insieme di caratteristiche che identificano l'individuo — e all'identità digitale, ovvero la proiezione nel mondo digitale di un individuo reale⁴⁷.

La profilazione è da tempo oggetto di molteplici provvedimenti del Garante per la protezione dei dati personali⁴⁸ e attualmente tale fattispecie è espressamente disciplinata nel GDPR, il quale

⁴⁵ Il processo di profilazione è attualmente definito dall'art. 4, par. I, n. 4, Reg. 2016/679/UE. A livello internazionale, già la Convenzione di Strasburgo del 1981 garantisce il rispetto dei diritti e delle libertà fondamentali, e in particolare del diritto alla vita privata, nei confronti dell'elaborazione automatizzata dei dati di carattere personale di una persona fisica; tutela precisata e ampliata in ambito europeo dalla Dir. 95/46/CE. Cfr. Convenzione di Strasburgo sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, 28.01.1981, n. 108, in *www.admin.ch*. (ratificata in Italia con L. 28.01.1989, n. 98). In Italia, l'art. 14, codice *privacy*, prevede il divieto di trattamento automatizzato, ripreso poi nell'art. 8, Dichiarazione dei diritti in Internet, 28 luglio 2015, in *www.camera.it*.

⁴⁶ Il diritto all'identità personale è notoriamente il frutto dell'attività giurisprudenziale iniziata nella metà degli anni '70 del secolo scorso e che ha trovato il suo culmine nel riconoscimento operato dalla Suprema Corte di Cassazione nel noto "caso Veronesi" Cass. 22.06.1985, n. 3769, in *Foro it.*, 1985, I, pp. 2211 ss. con nota di R. PARDOLISI. La pronuncia ha sancito che nell'ordinamento giuridico italiano sussiste il diritto all'identità personale, in quanto riconducibile all'art. 2 Cost. e deducibile, in via analogica, dalla disciplina prevista per il

diritto al nome. Il diritto all'identità personale è stato definito dal Tribunale Supremo come interesse giuridicamente meritevole di tutela a non veder travisato o alterato all'esterno il proprio patrimonio intellettuale, politico, sociale, religioso, ideologico, professionale ecc.. Per un maggiore approfondimento sull'identità personale si rinvia a V. ZENO-ZENCOVICH, voce *Identità personale*, in *Dig. disc. priv.*, sez. civ., IX, Torino, 1995, p. 295, V. ZENO-ZENCOVICH, *Diritto all'identità personale*, in *Nuova giur. civ.*, 1985, I, pp. 654 ss. e G. FINOCCHIARO, voce *Identità personale*, in *Dig. disc. priv.*, IANNARELLI-ROOK BASILE-SACCO-SCALA (con la collaborazione di), sez. civ., Agg., Torino, 2010.

⁴⁷ PACILEO P., *Profilazione e diritto di opposizione*, in AA. VV., *La nuova disciplina europea della privacy*, a cura di S. SICA, V. D'ANTONIO e M.G. RICCIO, Milano, 2016, pp. 177 ss.

⁴⁸ Si ricorda, tra l'altro, *'Fidelity card' e garanzie per i consumatori. Le regole del Garante per i programmi di fidelizzazione*, provv. 24.02.2005, in *www.garanteprivacy.it*, che nello stabilire che le c.d. "carte di fedeltà" vanno rilasciate anche se il consumatore non intende acconsentire ad eventuali iniziative di profilazione o di *marketing*, evidenzia il dovere di informare i clienti delle grandi catene di negozi e di supermercati beneficiari di tali carte in maniera chiara

stabilisce come principio generale il divieto di profilazione, salvo che questa sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e il titolare del trattamento, sia autorizzata da una norma di diritto europeo o di uno Stato membro cui è sottoposto il titolare del trattamento ovvero — ed è questa l'ipotesi su cui si intende porre l'accento — si basi sul consenso esplicito dell'interessato⁴⁹. In particolare, nei casi in cui la profilazione sia conseguenza di specifica approvazione da parte dell'utente, ci si chiede se egli sia realmente consapevole di cosa sia e di quali siano le sue conseguenze. Da un punto di vista opposto, ovvero nei casi in cui il consenso non venga richiesto, ci si chiede entro che limiti sia possibile impedire la profilazione, dato che tale processo può anche prescindere dal consenso prestato dall'interessato qualora questo sia il risultato dell'elaborazione algoritmica di dati personali (profilazione appunto) per i quali l'utente aveva già esplicitamente acconsentito al trattamento⁵⁰. A tal proposito è di estrema rilevanza il diritto di opposizione dell'interessato in qualsiasi momento al trattamento dei suoi dati personali — inclusa la profilazione (art. 21 GDPR) — tutela che si

ed evidente sugli scopi per i quali i loro dati personali vengono raccolti e, se le informazioni personali vengono usate anche per costruire profili di consumatori, per ricerche di mercato o per *direct marketing*, essi devono esprimere il loro consenso. In tal senso anche il provvedimento del 09.05.2006 sulla *Profilazione della clientela di alberghi*, che sanziona una grande catena alberghiera italiana per illecita profilazione della clientela (in quanto non venivano informati gli interessati né richiesto il loro consenso) che aveva lo scopo di conoscere meglio il cliente e anticiparne le richieste, oltre che finalità pubblicitarie. A fare chiarezza sulla profilazione online sono state, poi, le *Linee guida in materia di trattamento di dati personali per profilazione on line*, 19.05.2015, n. 161, in *www.garanteprivacy.it*, che prevedono maggiori tutele per gli utenti e regole più chiare per coloro che svolgono attività di *profiling*, con particolare riguardo al dovere di fornire informazioni chiare e complete, richiedere il consenso degli interessati (revocabile in ogni momento) e garantire concrete tutele anche ai soggetti che non hanno un account online. Sugli interventi del Garante per la protezione dei dati personali nell'ambito della profilazione si rinvia a P. PACILEO, *op. cit.*, pp. 187 ss.. Attualmente il diritto di informazione dell'interessato — sia in merito al trattamento dei suoi dati personali e alle finalità del trattamento, che relativamente alla profilazione e alle sue conseguenze — è

richiamato nel cons. 60, Reg. 2016/679/UE.

⁴⁹ Art. 22, Reg. 679/2016/UE. La Queen Mary University of London si è occupata di profilazione in uno studio sull'impatto delle tecniche di *machine learning* per profilare utenti nell'ambito del GDPR. L'obiettivo del lavoro è quello di dimostrare che i trattamenti automatizzati (compresa la profilazione) tramite *machine learning* possono essere conformi ai principi di liceità, correttezza e trasparenza del trattamento dei dati personali, distinguendo tra *discrimination as classification* o *prioritization as information*, che sono il cuore della *machine learning*, *unfair discrimination* che comporta un trattamento pregiudizievole. D. KAMARINOU, C. MILLARD e J. SINGH, *Machine Learning with Personal Data*, Queen Mary University of London, School of Law, *Legal Studies Research paper* no. 247/2016, in *www.papers.ssrn.com*, 2016, pp. 14 ss..

⁵⁰ I.A. CAGGIANO, *Il consenso al trattamento dei dati personali*, *cit.*, pp. 3 ss., pone l'accento sulla forza dello strumento informatico che può attingere a un numero infinito di informazioni provenienti da fonti differenti — database, motori di ricerca, e-mail, *social network*, servizi di *cloud computing*, e le stesse *smart things* — e aggregare una quantità di dati elevatissima, producendone, così, di ulteriori. Il *dataset* risulta quindi composto da un'enorme quantità di dati che prendono il nome di *big data*.

affianca al diritto di essere informato dal titolare del trattamento circa l'esistenza di un processo decisionale automatizzato, che comprende anche la profilazione stessa e — almeno in questa specifica ipotesi — al diritto di ricevere informazioni sulla logica utilizzata, l'importanza e le conseguenze di tale trattamento per l'interessato (art. 13, par. II, lett. *f.* e art. 14, par. II, lett. *g.*, GDPR)⁵¹. Infine, considerato il rischio per i diritti e le libertà dell'utente, il titolare del trattamento prima di procedere alla profilazione, deve effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (art. 35, par. II, GDPR).

I dati personali consentono di elaborare profili dettagliati degli utenti basati, tra l'altro, sui comportamenti, sulle abitudini, sulla salute, sull'età e sull'orientamento sessuale, politico o religioso degli stessi. In questo modo viene a crearsi un monitoraggio particolarmente invasivo della vita privata, che potrebbe persino produrre condizionamenti della libertà umana. Allo stesso tempo, però, la profilazione è molto importante per il mercato, in quanto i produttori sono in grado di individuare con precisione quali sono i prodotti maggiormente richiesti, in quali quantità⁵² e, inoltre, potrebbero migliorare gli stessi e ridurne i rischi sfruttando i dati personali degli utenti. Pertanto, sembrerebbe necessario individuare il giusto bilanciamento tra la profilazione dell'utente e la tutela dei suoi dati personali, con particolare riguardo al *digital profile*. In tal senso il GDPR disciplina espressamente la pseudonimizzazione, processo di dissociazione (teoricamente) irreversibile dei dati personali rispetto al titolare degli stessi, di modo che i dati non possano più essere attribuiti a un soggetto identificato o identificabile senza l'utilizzo di informazioni aggiuntive che vengono conservate separatamente e sono soggette a specifiche misure tecniche e organizzative atte a realizzare e mantenere la dissociazione⁵³. La pseudonimizzazione è una fattispecie diversa dall'anonimato, anche dal punto di vista delle tutele accordate⁵⁴. Infatti il dato viene reso anonimo mediante mascheratura di una serie di informazioni che potrebbero servire

⁵¹ In tal senso anche il cons. 60, 63 e 71 Reg. 2016/679/UE.

⁵² Provvedimento del Garante per la protezione dei dati personali del 16.12.2009, in www.garanteprivacy.it, in cui l'Autorità riconosce l'utilità della profilazione per le aziende, anche se impone ugualmente a queste ultime di ricorrere alla tecnica della profilazione solo in caso di specifico consenso da parte dell'interessato del trattamento. Allo stesso modo, G. PASCUZZI, *op. cit.*, pp. 71-72, ritiene che i dati vengano raccolti allo scopo di servire meglio i clienti a comprendere qual è la domanda del mer-

cato. Per tale motivo, i dati hanno un valore economico e il loro trattamento può essere metaforicamente paragonato al baratto, considerato che fornendo i dati personali gli utenti ottengono un servizio migliore ma, contemporaneamente, i titolari del trattamento possono controllare e prevedere l'andamento del mercato.

⁵³ Art. 4, par. I, n. 5, Reg. 2016/679/UE.

⁵⁴ La fattispecie dell'anonimato è disciplinata dalla Dir. 2016/681/UE, all'art. 12. Per un maggiore approfondimento G. FINOCCHIARO (a cura di), *Diritto all'anonimi-*

a identificare direttamente il soggetto cui si riferiscono, senza alcuna possibilità di reidentificazione, cosicché i dati anonimizzati cessano di essere oggetto di tutela. Per i dati pseudonimizzati, invece, c'è la possibilità di identificare gli interessati nel caso in cui si riesca ad accedere alle informazioni conservate separatamente e, per questo motivo, i dati rientrano nell'ambito applicativo delle norme sulla tutela dei dati personali⁵⁵. Tuttavia, appare opportuno segnalare che nella pratica non può escludersi in via assoluta la possibilità di identificare l'interessato del trattamento neanche quando i dati personali sono anonimi, considerando che le attuali tecniche di analisi, combinazione e raffronto di informazioni potrebbero consentire di identificare colui dei cui dati si tratta⁵⁶.

La tendenza verso la pseudonimizzazione, quale possibile soluzione alla profilazione di un utente identificato o identificabile, era già stata avallata nel 2012 dal Garante per la protezione dei dati personali che è intervenuto con un provvedimento sull'arricchimento dei dati personali della clientela nell'ambito dell'attività di profilazione. Si tratta di una tecnica profilatoria mediante la quale un *database* si arricchisce per aggregazione, incrociando i dati personali degli utenti con ulteriori informazioni derivanti dall'elaborazione statistica di una serie di dati (come quelli di natura geografica, socio-demografica e economica della popolazione presente in un determinato luogo di residenza). In tale provvedimento l'Autorità, ai sensi dell'art 24, co. 1, lett. g, cod. *privacy*, ha sancito che il trattamento di arricchimento dei dati personali della clientela all'interno del processo di profilazione può essere effettuato, anche senza richiedere il consenso dell'interessato, qualora abbia il fine di perseguire un legittimo interesse del titolare del trattamento e avvenga nel rispetto delle prescrizioni espressamente indicate nello stesso provvedimento (*ex art.*

mato, in *Trattato di dir. comm e dir. pubbl. dell'economia*, F. GALGANO (a cura di), XL-VIII, Bologna, 2008; Id., *Anonimato*, in *Digesto disc. priv.*, Sez. Civ., Torino, 2010; L. BOLOGNINI, E. PELINO e C. BISTOLFI, *Il regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016, pp. 74 ss..

⁵⁵ Cons. 26, Reg. 2016/679/UE: « [...] I dati personali sottoposti a pseudonimizzazione, i quali potrebbero essere attribuiti a una persona fisica mediante l'utilizzo di ulteriori informazioni, dovrebbero essere considerati informazioni su una persona fisica identificabile. [...] I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una per-

sona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato. Il presente regolamento non si applica pertanto al trattamento di tali informazioni anonime, anche per finalità statistiche o di ricerca ».

⁵⁶ Parere del Gruppo di lavoro per la protezione dei dati personali, sulle tecniche di anonimizzazione, 10.04.2014, n. 5, in www.ec.europa.eu, ritiene che sia difficile creare dati effettivamente anonimi mantenendo tutte le informazioni necessarie per l'espletamento delle attività richieste. Cfr. anche D'ORAZIO R., *Protezione dei dati by default e by design*, in AA. VV., *La nuova disciplina europea della privacy*, op. cit., p. 91; L. BOLOGNINI, E. PELINO e C. BISTOLFI, op. cit., pp. 77 ss.

17, cod. *privacy*)⁵⁷. La prima delle prescrizioni prevede proprio la necessità che i *record* dei clienti non contengano dati personali ricollegabili a un utente e che essi siano codificati in modo da non consentire di risalire all'identità dell'interessato. Pertanto, vengono di fatto profilate diverse tipologie di clienti senza, però, poter risalire all'identità di ogni singolo profilo elaborato, in quanto pseudoanonimo⁵⁸. Difatti, anche i dati non identificativi possono rendere una descrizione alquanto esaustiva di un soggetto o di una determinata categoria di soggetti (c.d. *clusterizzazione*)⁵⁹, ottenendo lo scopo (o quasi) perseguito dalla profilazione ma senza ledere gli interessi dei soggetti dai quali i dati provengono. La sostituzione dei dati identificativi di un soggetto o di un *cluster* con uno pseudonimo consente di ricollegare a costui o al *cluster* più informazioni e di elaborarne un profilo dettagliato⁶⁰. Sul punto il considerando 29 del GDPR sancisce che la pseudonimizzazione dovrebbe essere incentivata anche relativamente ai *big data* — evidenziandone i vantaggi — in modo da processare elevate quantità di dati senza però violare la *data protection*. Per garantire tale protezione il considerando impone specifiche condizioni all'analisi generalizzata dei *big data*: l'adozione di misure tecniche e organizzative adeguate (come la *data protection by design* e la *data protection by default* di cui si dirà) e l'adozione di misure di sicurezza atte a garantire che le informazioni aggiuntive necessarie per l'identificazione siano conservate separatamente rispetto ai dati pseudonimizzati.

4. LA SCELTA DEL METODO DI INDAGINE: ANALISI COMPORTAMENTALE E STUDI EMPIRICI.

A questo punto una parentesi sul metodo di ricerca adottato appare necessaria, dato che i risultati raggiunti possono variare a seconda del metodo di indagine utilizzato.

L'obiettivo del presente lavoro è quello di analizzare la normativa sulla protezione dei dati personali generati, memorizzati e processati dai veicoli autonomi, con particolare riguardo al ruolo che assume il consenso dell'interessato. Partendo da un'analisi

⁵⁷ Arricchimento dei dati personali della clientela nell'ambito dell'attività di profilazione, provv. 15.05.2012, in www.garanteprivacy.it.

⁵⁸ Per completezza appare necessario segnalare che la pseudonimizzazione è solo una delle possibili misure di protezione dei dati personali in cui si concretizza il principio della *data protection by design*, essendo possibile prevederne altre come espressamente sancito nel cons. 28, Reg. 2016/679/UE.

⁵⁹ Tecnica di analisi dei dati personali volta a selezionare e raggruppare soggetti omogenei che può essere soggetta a operazioni di profilazione. Cfr. L. BOLOGNINI, E. PELINO e C. BISTOLFI, *op. cit.*, pp. 83-84.

⁶⁰ Ovviamente non è possibile generalizzare, stabilendo che tutti i processi di profilazione debbano essere pseudoanonimi ma occorre valutare caso per caso il contrapposto degli interessi contrapposti: da un lato quelli del titolare alla profilazione e dall'altro quello dell'interessato del trattamento a non essere profilato.

critica dello stato dell'arte, si tenterà di raggiungere due obiettivi: 1) in primo luogo, verificare se l'attuale normativa sia sufficiente per una regolamentazione completa e sistematica dei veicoli autonomi e in particolare degli aspetti relativi alla protezione dei dati personali e, 2) in secondo luogo, si valuterà se il consenso al trattamento dei dati personali sia realmente uno strumento di tutela funzionale al perseguimento dei fini stabiliti dall'attuale normativa europea in materia — il GDPR *in primis* — ovvero sia preferibile ricorrere ad altre forme di tutela. Durante l'indagine, inoltre, ci si soffermerà sulla consapevolezza e l'autodeterminazione dell'interessato che si trova a dover decidere se prestare o meno il consenso al trattamento dei propri dati personali.

Per condurre un'analisi di questo tipo è fondamentale ricorrere alle scienze psico-comportamentali, nonché a casi pratici e simulazioni tecniche. Per questo motivo, il metodo di ricerca adottato è a carattere misto, avvalendosi non solo del materiale tradizionale afferente all'area giuridica, ma anche di studi comportamentali e di analisi empiriche a carattere interdisciplinare⁶¹. Nel XXI secolo — specialmente ove si abbia riguardo a settori del diritto in cui la tecnologia ha inciso fortemente — neanche gli studi di area giuridica possono più essere affrontati secondo un'impostazione metodologica meramente tradizionale, cioè limitandosi ad analizzare, più o meno criticamente, il materiale normativo, giurisprudenziale e dottrinale esistente. Il metodo tradizionale, invero, tende a produrre un andamento metodologico circolare e il lavoro di ricerca scientifica rischia di perdere di ogni utilità riducendosi, a volte, a mera ripetizione di quanto già detto. Al contrario, la ricerca dovrebbe essere lineare, con un punto di partenza e un obiettivo da raggiungere, per contribuire realmente all'avanzamento dello stato dell'arte⁶².

A proposito delle scienze psico-comportamentali, per indagare il comportamento dell'utente che si trova a dover fornire il consenso al trattamento dei propri dati personali dopo aver letto la relativa informativa, è estremamente importante partire dalla *human-*

⁶¹ Già da qualche tempo, una parte della letteratura ha rilevato che in un determinato contesto, caratterizzato dal coinvolgimento di diversi settori disciplinari della scienza e non solo dal diritto, la ricerca scientifica non può essere condotta utilizzando una prospettiva meramente teorica. Al contrario, risulta più opportuno ricorrere ad analisi empiriche e basarsi su *case study*. Cfr. A. MONTELERO, *Data protection, e-ticketing, and intelligent system for public transport*, in *International Data Privacy Law*, vol. 5, IV, 2015, p. 310; A. WOOD, D. R. O'BRIEN e U. GASSER, *Privacy and open data Research Briefing*, in Berkman Klein Cen-

ter's paper series of the Harvard University, *Translating Research for Action: Ideas and Examples for Informing Digital Policy*, 2016, p. 4. Per un approfondimento di carattere pratico sugli studi empirici si rinvia all'*Empirical Research Services* della Harvard Law School, in <http://hls.harvard.edu/library/empirical-research-services/>.

⁶² L. GATT, R. MONTANARI e 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.*, 2017, II, pp. 337 ss.

*robot interaction (HRI) analysis*⁶³ per poi verificare l'efficacia della normativa esistente⁶⁴. Si tratta di un'analisi comportamentale, basata sulla psicologia cognitiva, della relazione che intercorre tra l'uomo e il *robot* (il veicolo autonomo nel caso oggetto del presente lavoro). I risultati ottenuti dalla *HRI analysis* dovranno poi essere approfonditi da un punto di vista giuridico per valutare l'efficacia della normativa europea per la tutela dei dati personali⁶⁵ oppure l'eventuale necessità di modificarla o di introdurne una *ad hoc*, in una prospettiva *de iure condendo*.

Infine, occorre segnalare che la tecnologia non è qui solo oggetto di studio. Essa è anche strumento utilizzato per l'analisi del comportamento umano, condotta grazie all'ausilio di diversi strumenti tecnologici (*eye tracker*, *gaze plot*, *heatmap*, ecc.), nonché fondamento della tecnoregolazione che interviene in ausilio della regolamentazione normativa per tutelare i dati personali degli utenti (come nel caso della c.d. *data protection by design*)⁶⁶.

⁶³ La HRI — sottocategoria della *human machine interface (HMI)* — risulta fondamentale sia per l'individuazione dei diversi livelli di automazione che per i livelli di connessione dei veicoli, dato che questi sono direttamente proporzionali all'incremento dell'automazione. Sulla base di tale studio comportamentale è possibile valutare l'efficacia della normativa e l'effettività delle tutele in essa contenute, traendo le dovute conclusioni. Per uno studio più approfondito della HMI si rinvia a D. SIDOBRE ET AL., *Human-Robot Interaction*, in SICILIANO B. (a cura di), *Advanced Bimanual Manipulation, Springer Tracts in Advanced Robotics*, vol. 80, Heidelberg, 2012, pp. 123 ss.. Sul diritto cognitivo in generale e sullo studio comportamentale L. ARNAUDO, *Diritto cognitivo. Prolegomeni a una ricerca*, in *Politica dir.*, 2010, pp. 101 ss.; B. LURGER, *Empiricism and Private Law: Behavioral Research as Part of a Legal-Empirical Governance Analysis and Form of New Legal Realism*, in *Aust Law Jour.*, 2014, p. 19 ss..

⁶⁴ In proposito, si segnala che nel 2016 il Living Lab Utopia dell'Università Suor Orsola Benincasa di Napoli, su commissione di un importante partner tecnologico, ha condotto un esperimento di analisi comportamentale con valutazione giuridica dei risultati al fine di considerare l'efficacia della vigente normativa europea sul trattamento dei dati personali (e in particolare sul consenso), rientrante nel progetto *Privacy and Internet of Things: a behavioural and legal approach*, diretto dalla Prof.ssa Lucilla Gatt e vice-diretto Prof.ssa Ilaria Amelia Caggiano. L'esperimento è stato realizzato su un campione di 97 soggetti volontari a cui è

stato richiesto di interagire con un dato sistema operativo (installare il sistema, scaricare un'applicazione, navigare in internet, ecc.). È stata analizzata la consapevolezza degli utenti e la loro conoscenza del processo di trattamento dei dati personali, tramite questionari e tecnologie di misurazione del comportamento durante lo svolgimento dei *tasks* e, in special modo, durante il conferimento del consenso (per verificare il potere di autodeterminazione del singolo). In particolare, per quantificare il grado di consapevolezza e conoscenza della materia *privacy* sono stati sottoposti all'utente dei questionari misti a risposta aperta e multipla; quanto all'analisi comportamentale, per misurare l'attenzione, si è fatto ricorso alle rappresentazioni grafiche *heatmap*, per calcolare il tempo di esecuzione dei *tasks* si sono cronometrate le tempistiche, per analizzare l'ordine di lettura all'interno delle singole schermate sono stati utilizzati *gaze plot*, per valutare l'usabilità, infine, sono stati presi in considerazione l'ordine di lettura all'interno delle schermate e le tempistiche di esecuzione dei *tasks*. I risultati del progetto saranno brevemente presentati nel par. VI. Cfr. L. GATT, R. MONTANARI e I.A. CAGGIANO, *op. cit.*, pp. 338 ss.; I.A. CAGGIANO, *A quest for efficacy in data protection: a legal and behavioural analysis, Working Paper* n.10/2017, pp. 11 ss.

⁶⁵ L. GATT, R. MONTANARI e I.A. CAGGIANO, *op. cit.*, p. 342.

⁶⁶ M. ERIKSSON, *The normativity of automated driving: a case study of embedding norms in Technology*, in *Info. & Comm. Tech. L.*, vol. 26, issue 1, 2017, pp. 46 ss.. In tal senso anche G. PASCUZZI, *op. cit.*, pp.

5. LA NECESSITÀ DI UNA DISCIPLINA NORMATIVA PER I VEICOLI AUTONOMI.

Le spinte europee per l'introduzione di una disciplina normativa sulla robotica sono numerose. Da ultimo, con la risoluzione del febbraio 2017, il Parlamento europeo ha richiesto alla Commissione europea di presentare una proposta legislativa concernente norme di diritto civile sulla robotica e l'intelligenza artificiale, al fine di dirimere le principali questioni prevedibili nei prossimi 10-15 anni, nonché atti non legislativi (specificamente linee guida e codici di condotta), tenendo conto della Carta sulla robotica allegata alla risoluzione⁶⁷. Inoltre, l'Europarlamento ritiene che il settore automobilistico sia quello in cui si avverte maggiormente la necessità di norme efficaci, applicabili a livello europeo e internazionale, al fine di garantire lo sviluppo anche transfrontaliero dei veicoli autonomi, sfruttandone il potenziale economico e beneficiando dei vantaggi che derivano da tali tecnologie⁶⁸. Anche nella Dichiarazione di Amsterdam sulla cooperazione nel campo della guida connessa e automatizzata⁶⁹ è stata sancita la necessità di sviluppare e mantenere un programma, comune con gli altri Stati europei, per sostenere gli obiettivi prefissati e porre rimedio alle problematiche che derivano dallo sviluppo di tale nuova tipologia di guida⁷⁰.

92-93, conclude la discussione sulla *privacy* nell'Internet degli oggetti dichiarando che l'avvento dell'era digitale comporta diversi cambiamenti, tra cui sicuramente quello del conferimento alla tecnologia stessa del compito di garantire il rispetto delle norme sul trattamento dei dati personali. T.E. FROSINI, *Rappresentanza e legislazione nell'età della globalizzazione*, in *Annuario di diritto comparato e di studi legislativi*, vol. VIII, Napoli, 2017, pp. 296 ss., si focalizza sul mutamento delle caratteristiche e della funzione della legge con l'avvento della globalizzazione. L'autore ritiene che la legge sia entrata in una fase di dissolvenza dato che, nell'era moderna era una legge rigida, mentre la legge post moderna è molto più flessibile. Di conseguenza, è mutato l'uso della legge, attualmente soggetta ad una continua opera di interpretazione, « che può arrivare a ribaltarne la lettera per favorire lo spirito ».

⁶⁷ Risoluzione del Parlamento europeo, *cit.*, punto n. 51.

⁶⁸ *Ivi*, punto n. 25. In merito alle norme internazionali, viceversa, il Parlamento europeo sostiene che non sia urgente la modifica sostanziale delle norme di diritto internazionale privato sugli incidenti stradali ma appare opportuno semplificare l'attuale duplice sistema per l'individuazione della legge applicabile: Reg. 2007/364/CE sulla legge

applicabile alle obbligazioni extracontrattuali (c.d. Regolamento Roma II) e Convenzione dell'Aja del 4 maggio 1971 sulla legge applicabile in materia di incidenti della circolazione stradale. Al contrario, per consentire la guida senza conducente, nella risoluzione si ritiene opportuna la modifica della Convenzione di Vienna sul traffico stradale dell'8 novembre 1968. Infatti, anche alla luce dell'emendamento del 2016, la Convenzione di Vienna prevede che le funzioni di guida automatica siano ammesse solo qualora possano essere disattivate manualmente dal conducente in qualsiasi momento; ciò implica che le auto a guida autonoma devono necessariamente prevedere lo spegnimento del sistema di pilota automatico. Infine, il Parlamento sottolinea che dovrebbero attuarsi il più rapidamente possibile gli obiettivi della Dichiarazione di Amsterdam e che dovrebbero applicarsi anche alla robotica le condizioni di cui al Reg. 2009/428/CE sul controllo delle esportazioni, del trasferimento, dell'intermediazione e del transito di prodotti a duplice uso. Cfr. *Ivi*, punto nn. 60 ss.; DEKRA, *Road safety report* 2017, in www.dekra.it, p. 81.

⁶⁹ V. nota n. 11.

⁷⁰ Gli obiettivi prefissati dalla Dichiarazione di Amsterdam riguardano l'elaborazione (preferibilmente entro il 2019) di un *framework* europeo applicabile alla guida

Giungendo alla protezione dei dati personali — su cui si incentra il presente contributo — nell'ordinamento giuridico italiano la “pacifica rivoluzione della *privacy*”⁷¹ ha avuto inizio con l'entrata in vigore della legge n. 675/1996⁷², che ha attribuito a ogni individuo il potere di governare le informazioni che lo riguardano. La legge del '96 è stata abrogata dall'attuale Codice in materia di protezione dei dati personali il quale, a sua volta, dovrà essere adeguato al nuovo GDPR, entrato in vigore il 24 maggio 2016 e applicabile in via diretta in tutti i Paesi membri dell'Unione europea a partire dal 25 maggio 2018⁷³. Anche la risoluzione europea rileva la centralità del problema della tutela dei dati personali e il Parlamento è chiaro nello stabilire che le norme di diritto civile sulla robotica devono essere coerenti sia con GDPR, che con gli artt. 7 e 8 della Carta di Nizza e con l'art. 16 del Trattato sul funzionamento dell'Unione europea (TFUE)⁷⁴, anche se altri aspetti concernenti la protezione dei dati devono ancora essere affrontati⁷⁵. A proposito del GDPR, nella

autonoma e connessa. Essi hanno il fine di beneficiare appieno dei vantaggi della guida autonoma (miglioramento della sicurezza, della salute, delle condizioni del traffico stradale e dell'inquinamento ambientale), adottare un approccio fondato sul *learning by experience* (anche grazie a una cooperazione transfrontaliera), rafforzare la posizione dell'industria europea nel mercato globale e, infine, ma non per questo meno importante, assicurare la protezione dei dati personali. In tema di sicurezza si veda la *Joint agenda della Dichiarazione di Amsterdam*, lett. E, e la *Federal Automated Vehicles Policy*, U.S. Department of Transportation, settembre 2016, in www.transportation.gov.

⁷¹ Relazione 2004 del Garante per la protezione dei dati personali, Discorso del Presidente Stefano Rodotà, in www.garanteprivacy.it, 2005, p. 1 ss..

⁷² L. 31.12.1996, n. 675 sulla tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali, abrogata dall'attuale Codice in materia di protezione dei dati personali (c.d. codice *privacy*, d.lgs. 30.06.2003, n. 196, in www.normattiva.it).

⁷³ Ai sensi dell'art. 99, Reg. 2016/679/UE, a partire dal 25 maggio 2018 la normativa interna di ogni stato membro dovrà essere conforme al Regolamento, mentre le Direttive dovranno essere recepite dagli Stati membri entro i successivi due anni; F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, tomo II, *Il regolamento europeo 2016/679*, Torino, 2016, p. 14, evidenzia che le legislazioni europee e

nazionali incompatibili con il Regolamento devono essere adeguate a quest'ultimo, salvo che si tratti di materie oggetto di esplicita competenza legislativa statale ovvero siano norme europee che non devono essere sostituite ma bilanciate con il nuovo Regolamento (ad esempio il Cons. 42, Reg. 2016/679/UE che richiama la Direttiva 93/13/CE, la quale definisce le clausole abusive nei contratti del consumatore e chiarisce le modalità attraverso le quali devono essere fornite le informazioni al fine di ottenere un consenso consapevole).

⁷⁴ Il Trattato di Lisbona, modificando l'art. 6 del Trattato sull'Unione europea (TUE), ha innalzato la Carta di Nizza al rango dei Trattati e ciò ha comportato l'inclusione nelle fonti primarie del diritto dell'Unione europea anche delle norme della Carta che riconoscono alla protezione dei dati personali natura di diritto fondamentale. Inoltre, lo stesso Trattato di Lisbona ha modificato il Trattato sul funzionamento dell'Unione europea (TFUE), introducendo esplicita menzione del diritto alla protezione dei dati personali all'art. 16. Cfr. AIELLO G. F., *op. cit.*, pp. 4 ss.; Trattato di Lisbona, che modifica il Trattato sull'Unione europea e il Trattato che istituisce la Comunità europea, 13.12.2007, C 306/01, in www.eur-lex.europa.eu, (ratificato in Italia con L. 02.08.2008, n. 130 ed entrato in vigore l'1.12.2009).

⁷⁵ D'ORAZIO R. *op. cit.*, pp. 79 ss., precisa che — nonostante il GDPR recepisca soluzioni da tempo discusse — non può ritenersi del tutto superata la problematicità di alcuni profili connessi alla protezione

risoluzione parlamentare si invita la Commissione a garantire che siano rispettati i principi della protezione dei dati personali fin dalla fase di progettazione (c.d. *data protection by design*) e per impostazione predefinita (c.d. *data protection by default*), minimizzando il trattamento dei dati e limitandone le finalità ⁷⁶.

Sulla base di quanto fin qui esposto, è forte la necessità di introdurre una normativa europea (o meglio ancora internazionale) che regolamenti i veicoli autonomi in conformità con le norme già esistenti che, tuttavia, non risultano del tutto adeguate ⁷⁷. Percorrendo tale strada, la prima domanda cui occorre rispondere è se sia sufficiente l'introduzione di una normativa sulla robotica in generale ovvero se sia più opportuno prevedere una disciplina *ad hoc* per i principali settori della robotica tra cui, sicuramente, quello dei veicoli autonomi ⁷⁸. La seconda soluzione appare preferibile — oltre che in linea con la risoluzione parlamentare — considerando che i settori della robotica sono così

dei dati personali a causa delle rispettive implicazioni giuridiche e politiche.

⁷⁶ Risoluzione del Parlamento europeo, cit., punti nn. 19 ss.

⁷⁷ A. DAVOLA e R. PARDOLESI, *In viaggio col robot: verso nuovi orizzonti della r.c. auto ("driverless")?*, op. cit., pp. 617 ss., evidenziano come l'integrazione delle nuove tecnologie nella vita quotidiana sia sempre più massiccia, richiedendo un approfondimento e una regolamentazione delle conseguenze derivanti dall'utilizzo dei robot e, in generale, dell'intelligenza artificiale. C. PERLINGERI, *L'incidenza dell'utilizzazione della tecnologia robotica nei rapporti civilistici*, in *Rassegna di diritto civile*, IV, 2015, pp. 1239-1240, rileva che la robotica sollecita l'elaborazione di nuove disposizioni normative, menzionando — a titolo esemplificativo — il problema della responsabilità civile con riguardo a comportamenti che cagionano ad altri un danno ingiusto. R.H. WEBER, op. cit., pp. 26 ss., mette in risalto la necessità di introdurre e implementare un appropriato *legal framework* per la protezione della sicurezza e della *privacy* nell'IoT. Più propriamente, egli — escludendo la possibilità di non introdurre alcuna regolamentazione — si interroga sul modello normativo preferibile: regolamentazione nazionale tradizionale, accordi internazionali o autoregolamentazione. Il terzo modello è quello che attualmente disciplina l'IoT (attraverso *standards*, linee guida e buone pratiche informative); questo, però, non risulta sufficiente per una completa regolamentazione e, ad avviso dell'autore, la migliore soluzione sembrerebbe quella di introdurre principi chiave applicabili a li-

vello internazionale (e non soltanto europeo), opportunamente integrati dal diritto sostanziale. *European Research Cluster on the Internet of Things (IERC)*, op. cit., pp. 25 ss., infine, ritiene che l'IoT abbia bisogno di essere costruito in modo da assicurarne un facile e sicuro utilizzo per ottenere la fiducia degli utenti e sfruttare al massimo il suo potenziale; gli *open standards* sembrerebbero essere lo strumento più adeguato per il perseguimento di tali obiettivi.

⁷⁸ Il termine *robot* deriva dal ceco *robota*, che letteralmente vuol dire lavoro (forzato) ed è stato utilizzato per la prima volta da Karel Čapek nel suo dramma fantascientifico *Rossum's Universal Robots* (R.U.R.) del 1920 per fare riferimento agli automi che lavoravano al posto degli operai. Da una ricerca condotta sulle principali enciclopedie e dizionari in Europa è emerso che non c'è generale consenso sulla definizione di *robot*. Ad esempio l'Enciclopedia Britannica lo considera come « any automatically operated machine that replaces human effort, though it may not resemble human beings in appearance or perform functions in humanlike manner »; il Vocabolario Treccani online lo definisce « apparato meccanico ed elettronico programmabile, impiegato nell'industria, in sostituzione dell'uomo, per eseguire automaticamente e autonomamente lavorazioni e operazioni ripetitive, o complesse, pesanti e pericolose ». Tali definizioni superano l'iniziale idea di *robot* secondo la quale si trattava di una macchina con sembianze umane (*human-like*), tanto che anche i veicoli autonomi rientrino pacificamente in tale nozione. In tal senso A. SANTOSUOSSO, C. BOSCARATO e F.

numerosi e diversi tra loro che una normativa generica rischierebbe di non riuscire a regolare tutti i casi specifici di un determinato settore, lasciando inalterato il sentimento di incertezza e inadeguatezza della normativa che attualmente si avverte. Inoltre, tale esigenza è ancora più evidente nella fase di transizione in cui ci troviamo — caratterizzata da un'automazione parziale — dato che, fino a quando non si raggiungerà un'automazione totale, le differenze tra le tipologie di *robot* saranno ben evidenti. Basti pensare ai droni in contrapposizione ai veicoli autonomi, che fino al raggiungimento della *high automation* saranno caratterizzati da una sostanziale differenza: i primi sono dispositivi a pilotaggio remoto i secondo sono a pilotaggio diretto.

Sono numerosi gli Stati che iniziano a considerare una legislazione specifica per le *self-driving cars*. Negli Stati Uniti d'America, la *National Highway Transportation Safety Administration* (NHTSA) ha riconosciuto i *Self-Driving System* (SDS) come *driver* del veicolo e ha dichiarato che provvederà all'integrazione in tal senso della disciplina normativa sulla sicurezza stradale, aggiornando il *Federal Register* ⁷⁹. Nel vecchio continente, invece, la Germania è stata la prima e unica nazione ad aver già approvato una normativa sui veicoli autonomi ⁸⁰. In Gran Bretagna, poi, è stato presentato un progetto di legge che però non è stato

CAROLEO, *Robot e diritto: una prima ricognizione*, in www.pluriscedam.utetgiuridica.it, 2012, pp. 1 ss., che suggeriscono di considerare il *robot* come macchina che svolge autonomamente un lavoro. C. PERLINGERI, *op. cit.*, pp. 1236 e 1243, invece, si interroga sulla riconducibilità dei *robot* nella categoria dei soggetti di diritto piuttosto che nell'alveo delle *res*, ma conclude in senso negativo ponendo l'accento sul valore della persona umana racchiuso nei principi costituzionali oltre che nelle norme di diritto positivo. Il Parlamento europeo, poi, dopo aver dichiarato l'importanza di elaborare una definizione europea di *robot*, considera l'opportunità di dividerlo anche in sottocategorie, tenendo conto di alcune caratteristiche: la capacità di acquisire autonomia, la capacità di apprendimento, la forma del supporto fisico, la capacità di adeguare il proprio comportamento all'ambiente circostante. Cfr. Risoluzione del Parlamento europeo, *cit.*, allegato alla risoluzione.

⁷⁹ Ciò è stato il risultato di una lettera che la NHTSA, il 4 febbraio 2016, ha inviato a Chris Urmson, allora direttore del progetto Google *self-driving car* (oggi confluito in Waymo), rispondendo alle richieste fatte da Google sulla regolamentazione della circolazione stradale dei veicoli autonomi.

Cfr. www.nhtsa.gov. Ad oggi sono trentatré gli stati che hanno introdotto una *legislation related to autonomous vehicles*. Per approfondire il tema si rinvia al sito internet della *National Conference of State Legislatures* in www.ncsl.org.

⁸⁰ Il 20 febbraio 2017, il Consiglio federale tedesco ha approvato il disegno di legge avente a oggetto la guida autonoma, che modifica la legge sulla circolazione stradale. Tuttavia, anche con l'introduzione della nuova normativa la responsabilità aquiliana è in capo al proprietario del veicolo in caso di sinistro e viene configurata come responsabilità oggettiva per incidenti dovuti al malfunzionamento del veicolo, prevista dal par. 7. Il par. 12, invece, specifica i massimali del risarcimento del danno, che sono aumentati in ragione del fatto che vi è quasi una totale assenza di dati relativi a incidenti causati da veicoli autonomi. Il *corpus* normativo è stato studiato per un livello di automazione intermedio (livello 3 principalmente) in cui al posto di guida deve esserci sempre una persona fisica, la quale può svolgere altre attività ma deve essere in grado di riassumere tempestivamente il controllo del veicolo in caso di richiesta da parte del sistema di guida oppure qualora si renda conto che siano venuti meno i presup-

approvato⁸¹. A livello europeo, come già chiarito, manca una regolamentazione *ad hoc* anche se vi sono diverse normative di settore che, interpretate in via analogica, potrebbero essere applicate alle questioni concernenti la protezione dei dati personali nei veicoli autonomi, fino a quando non sarà introdotta una specifica normativa europea⁸².

Cosa dovrebbe prevedere un'eventuale normativa europea per la regolamentazione dei veicoli autonomi? Quali sono i principali

posti per la guida autonoma (par. 1b). A tutela del conducente (definito come colui che è in grado di attivare e disattivare la modalità di guida autonoma), però, è stato previsto un dispositivo di memorizzazione dei dati installato sul veicolo che registra come il sistema di bordo stia funzionando, in modo da consentire al produttore di utilizzare quei dati per renderlo più sicuro e, in caso di incidente, di stabilire chi sia il soggetto realmente imputabile. Certamente ritorna la questione della protezione dei dati personali, tutelati e disciplinati espressamente nel par. 63 il quale prevede che l'autoveicolo debba raccogliere i dati relativi al funzionamento del sistema di guida in modo da essere in grado di valutare la necessità di inoltrare al conducente la richiesta di intervento. Cfr. *Entwurf eines Gesetzes zur Änderung des Straßenverkehrsgesetzes* (Disegno di legge sulla modifica della legge sul traffico stradale), 20.02.2017, n. 18/11300, in www.bundestag.de. Per un maggiore approfondimento sulla modifica della legge tedesca sul traffico stradale v. A. DAVOLA e R. PARDOLESI, *In viaggio col robot: verso nuovi orizzonti della r.c. auto* ("driverless")?, *op. cit.*, pp. 622-623.

⁸¹ *Vehicle technology and aviation bill 2016-17*, 22.02.2017, n. 143, in www.parliament.uk, che sembrerebbe propendere per l'attribuzione della responsabilità civile extracontrattuale in capo alla compagnia assicurativa ovvero al proprietario del veicolo in caso di incidente automobilistico. Precisamente la sezione 2 fa riferimento (forse impropriamente) alla responsabilità della compagnia assicurativa, probabilmente volendo sostenere che, anche se di fatto sarebbe imputabile il conducente, i danni sono risarciti dalla sua compagnia assicurativa, nell'ipotesi in cui il veicolo autonomo che aveva causato l'incidente — arrecando un danno a terzi — era assicurato al momento del sinistro; nell'ipotesi in cui, invece, la *self-driving car* non era assicurata, ne è responsabile il proprietario. Inoltre, la sezione 3, disciplina il concorso di colpa (con la compagnia assicurativa o con il proprietario del veicolo) del danneggiato ovvero del guidatore; nel primo caso,

se l'azione del danneggiato ha causalmente contribuito al verificarsi del sinistro, viene ridotta l'obbligazione risarcitoria in ottemperanza al *Law Reform (Contributory Negligence) Act 1945*, mentre nel secondo caso l'assicuratore o il proprietario del veicolo vengono interamente manlevati dalla propria responsabilità, se il guidatore ha negligenziosamente consentito l'attivazione del sistema di guida autonoma in circostanze inappropriate. La sezione 4, invece, prevede espressamente due casi di esonero di responsabilità per la compagnia assicurativa: a) nel caso di modifiche del sistema operativo del veicolo effettuate direttamente dall'assicurato o quando questi ne era comunque consapevole, ovvero b) nel caso in cui non sia stato aggiornato il *software* di guida da parte dell'assicurato che aveva il compito di provvedervi, come previsto nel contratto di assicurazione. Infine, ai sensi della sezione 5, nel caso in cui l'incidente sia stato causato da un soggetto terzo, sia l'assicuratore che il proprietario del veicolo hanno il diritto di agire contro di lui. Per una disamina più approfondita del *Vehicle technology and aviation bill 2016-17* v. A. DAVOLA e R. PARDOLESI, *In viaggio col robot: verso nuovi orizzonti della r.c. auto* ("driverless")?, *op. cit.*, pp. 621-622.

⁸² Oltre al GDPR, si segnalano: sul sistema informativo e-call il Reg. 2015/758/UE, la Dec. 2014/585/UE e il Reg. 2013/305/UE; sull'*Intelligent transport Systems* (ITS) la Dir. 2010/40/UE e i regolamenti delegati: sulle comunicazioni elettroniche la Dir. 2002/22/CE, la Dir. 2002/21/CE, la Dir. 2002/20/CE, la Dir. 2002/19/CE e la Dir. 2002/58/CE (che potrebbe essere sostituita dalla 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), tutti consultabili su www.eur-lex.europa.eu. Sempre in Europa, inoltre, vi sono diverse iniziative che mirano a disciplinare la robotica e le nuove tecnologie in generale. Infatti, oltre alla Relazione del Parlamento europeo sulle norme di diritto civile sulla robotica, alla Dichiarazione di Amsterdam, alla proposta di re-

aspetti da analizzare e le soluzioni auspicabili? Tali domande richiedono una dissertazione più ampia che ci si ripropone di affrontare in altra sede mentre in questa s'intende esaminare i profili connessi alla tutela dei dati personali, dividendo tra regole sulla dazione del consenso al trattamento dei dati personali nei *connected vehicles* (v. *infra* par. VI) e regole sulla progettazione di tali veicoli, in linea con la c.d. *privacy by design* (v. *infra* par. VII).

6. LA (NON) RILEVANZA DEL CONSENSO AL TRATTAMENTO DEI DATI PERSONALI.

Il consenso dell'interessato, così come argomentato nel considerando 32 del GDPR, viene valorizzato in chiave positiva⁸³. In particolare, nel GDPR, la regola è quella del consenso espresso (cons. 32, GDPR) e l'eccezione è quella del consenso esplicito, richiesto solo con riguardo ai dati sensibili (art. 9, GDPR), alla profilazione (art. 22, GDPR) e al trasferimento dei dati presso un Paese terzo o un'organizzazione internazionale (art. 49, par. 1, lett. a, GDPR). Tuttavia, la differenza tra consenso espresso ed esplicito non è chiara e sembrerebbe che il consenso esplicito non sia altro che un consenso espresso caratterizzato da una maggiore determinatezza nel contegno⁸⁴.

Il cons. 32, peraltro, ammette qualsiasi atto positivo che indichi chiaramente la volontà dell'interessato di acconsentire al trattamento come avviene, ad esempio, con la selezione di un'apposita casella in un sito web. Tale modalità di prestazione del consenso era già stata avallata dal Garante italiano per la protezione dei dati personali⁸⁵ e, attualmente, è molto frequente nelle ipotesi di consenso richiesto attraverso mezzi elettronici dove addirittura si ammettono determinate azioni che sembrano più affini alla nozione di comportamento concludente piuttosto che alla espressa

golamento sulle comunicazioni elettroniche e alla Comunicazione della Commissione europea sulla revisione della strategia per il mercato unico digitale, già menzionate, si richiamano la COM/2016/0766 sui *Cooperative Intelligent transport Systems* (C-ITS), Letter of Intent on the testing and large scale demonstrations on Connected and Automated Driving (CAD), Roma, 23.03.2017, che mira alla cooperazione nel quadro di esperimenti transfrontalieri relativi alla sicurezza stradale, all'accesso ai dati, alla qualità e affidabilità dei dati, alla connettività e alle tecnologie digitali, l'EU-U.S. *Privacy Shield* C(2016) 4176, che disciplina il trasferimento di dati personali a fini commerciali tra Europa e Stati Uniti d'America, e l'*High Level Group for the automotive industry* (GEAR), C(2015) 6943, che è

molto attivo nell'ambito dell'automazione.

⁸³ Non è richiesta la forma scritta del consenso, a differenza di quanto espressamente previsto in Italia per i dati sensibili, ai sensi dell'art. 26, cod. privacy.

⁸⁴ In tal senso I.A. CAGGIANO, *Il consenso al trattamento dei dati personali*, cit., p. 11.

⁸⁵ Il quale ha introdotto il concetto di *positive option*, non consentendo l'impiego di quei moduli e formulari che facevano discendere il consenso dell'interessato dal fatto che non avesse selezionato l'opzione relativa al dissenso al trattamento dei dati personali. S. MAZZAMUTO, *Il principio del consenso e il potere della revoca*, in AA. Vv., *Libera circolazione e protezione dei dati personali*, R. PANNETTA (a cura di), Tomo I, Milano, 2006, pp. 1015-1016.

manifestazione della volontà. Riprendendo l'esempio citato del sito web, in alcun caso non è richiesta la selezione di una casella ma, nel *banner* che compare nella *home page* richiedendo il consenso al trattamento, è previsto che lo stesso possa essere fornito semplicemente continuando a navigare sul sito Internet, il che non configura esattamente un atto positivo inequivocabile. Inoltre, non sono pochi i casi in cui il consenso non viene chiesto affatto, come si evince da ultimo nella relazione introduttiva alla proposta di Regolamento c.d. *e-privacy*, in cui il Parlamento europeo e il Consiglio criticano la normativa della Direttiva 2002/58/CE sulle comunicazioni elettroniche in merito al consenso per non aver realizzato gli obiettivi prefissati nella Direttiva stessa. Infatti, gli utenti finali si trovano di fronte a richieste di accettare i marcatori (c.d. *cookie* di tracciatura) senza capirne il senso o in alcuni casi sono addirittura esposti ai *cookie* senza avervi prestato il consenso ⁸⁶.

Esaminando, poi, il comportamento degli utenti richiesti di prestare il consenso al trattamento dei propri dati personali per usufruire di un servizio, è stato evidenziato che questi acconsentono al trattamento quasi sempre e senza prestare attenzione all'informativa *privacy* ⁸⁷. Invero, il consenso al trattamento è il requisito necessario per poter accedere a determinati servizi,

⁸⁶ 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 (c.d. proposta di regolamento *e-privacy*), 10.01.2017, 2017/0003(COD), in www.eur-lex.europa.eu.

⁸⁷ V. *supra* nota n. 64 per la descrizione dell'esperimento *Privacy and Internet of Things: a behavioural and legal approach*. Quanto ai risultati, vi è una notevole discrepanza tra le risposte del questionario e il comportamento degli utenti: la maggioranza degli intervistati ha affermato di prestare molta attenzione al trattamento dei propri dati personali ma, in realtà, solo una piccola percentuale di questi ha disabilitato le impostazioni predefinite (che tutelano meno la *privacy*), più della metà degli utenti non hanno letto l'informativa al momento dell'installazione del sistema operativo e una gran parte degli utenti ritiene utile consentire la geo-localizzazione o il riconoscimento vocale. Tuttavia, quando gli utenti sono stati indotti a ritornare sul pannello di controllo per verificare se, alla luce del test effettuato, avevano intenzione di

modificare le impostazioni sulla *privacy*, tutti hanno agito in tal senso (ovviamente si trattava di un'operazione indotta ed era prevedibile il comportamento degli utenti). Cfr. I.A. CAGGIANO, *A quest for efficacy in data protection*, cit., pp. 13-14: « From the collected answers and users' activity observed, there is a general tendency to prefer operative choices that imply the simplest and shortest solution. Specifically, as to the information and management on data processing, users were revealed to have misunderstood the information provided, although they perceived themselves to be aware and able to manage the privacy setting commands. The experiment, although at its initial stage, shows that even those who care about their personal data generally do not pay attention to or outright disregard the privacy notice, even in a non-natural environment (the experiment) where subjects are specifically required to perform the task of reading the privacy policy. Consent to the processing of personal data is given simply following the activities to which the data processing is functional and it plays no role in decisions pertaining to daily activities, also considering that clauses on data

oppure a particolari funzioni degli stessi⁸⁸. Viene meno, così, l'effettivo potere di autodeterminazione dell'utente tramite la dazione del consenso, inteso come manifestazione dell'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano.

Addentrandosi nei meandri dell'*Internet of things*, quale spazio in cui avviene lo scambio dei dati personali e focalizzandosi sui dati scambiati tra *connected vehicles*, la questione si complica ulteriormente a causa della elevatissima quantità di dati processati⁸⁹. Difatti, se è vero che in alcune circostanze dove sono coinvolte le nuove tecnologie è difficile prevedere un consenso espresso (e ancora più quello esplicito), si può immaginare quanto sia ancora più complesso ottenere tale consenso da parte di coloro che si trovano a bordo di un veicolo autonomo. Appare quindi naturale domandarsi come e in che momento il proprietario del veicolo e gli eventuali passeggeri debbano essere informati sul trattamento dei propri dati personali, quale sia la forma del relativo consenso e se questo debba essere fornito *una tantum* ovvero ogni volta che si utilizza la *self-driving car*.

La strada da seguire non può che essere quella dell'elaborazione di un *framework* di regole giuridiche, applicabile a livello europeo, che disciplini le modalità attraverso le quali tutelare gli utenti con particolare riguardo al trattamento dei propri dati personali generati, elaborati e processati dai veicoli connessi. Più dettagliatamente, sarebbe importante prevedere un'adeguata e funzionale informativa sul trattamento dei dati personali — come richiesto dal GDPR⁹⁰ — in modo che gli utenti sappiano esattamente quali siano le conseguenze del trattamento. L'informativa, per essere adeguata, non può corrispondere a un modello *standard* utilizzato per ogni tipologia di trattamento. Al contrario, questa deve essere chiara, specifica e facilmente comprensibile da

processing in the digital environment are consistently “take it or leave it”. [...] These studies collectively show that, in a more or less conscious manner, the information is not read and therefore the consent given is not consciously provided ».

⁸⁸ Si pensi banalmente ai servizi di ricerca e visualizzazione di mappe geografiche che forniscono indicazioni sulla strada da percorrere per raggiungere un determinato luogo, i quali, per individuare più rapidamente il percorso migliore da seguire, hanno bisogno di geo-localizzare l'utente. Nella gran parte dei casi l'utente acconsente a comunicare la propria localizzazione al fine di poter godere di un servizio più rapido e preciso. I principali servizi di questo tipo sono *Google maps*, *Apple Maps* e *Mappe*

di Windows. In merito alla necessità di trattare i dati personali per offrire *value-added service* v. J.W. BRYANS, *The Internet of Automotive Things: vulnerabilities, risks and policy implications*, in *Journal of Cyber Policy*, 2017, II, no. 2, pp. 190-191.

⁸⁹ W.K. HON, C. MILLARD, J. SINGH, *op. cit.*, p. 23.

⁹⁰ I contenuti dell'informativa sono elencati in modo tassativo negli artt. 13 e 14, Reg. 2016/679/UE. Quanto alle modalità, in ottemperanza al principio di trasparenza, il regolamento specifica le caratteristiche dell'informativa che deve avere forma concisa, trasparente, intelligibile per l'interessato ed essere facilmente accessibile. Occorre utilizzare un linguaggio chiaro e semplice ed eventualmente anche una visualizzazione grafica (Art. 12 e cons. 58., Reg. 2016/679/UE).

un utente medio che è, quindi, realmente informato dell'esistenza del trattamento e delle sue finalità, dell'eventuale profilazione e delle sue conseguenze, nonché dei suoi diritti, in conformità con i principi di trattamento corretto e trasparente, previsti nel GDPR. Solo in questo modo si può tentare di contrastare il forte disinteresse degli utenti per l'informativa⁹¹, in modo da renderli effettivamente edotti, tutelando sia i loro interessi che quelli dei titolari del trattamento a non incorrere in sanzioni per il mancato adempimento dell'obbligo di informazione dell'interessato.

Quanto al consenso dell'interessato, invece, l'ipotizzato *framework of rules* potrebbe superare (in tutto o in parte) il requisito del consenso, considerando che questo non risulta più uno strumento normativo che garantisce l'effettività della tutela della sfera personale⁹². Infatti, stanno aumentando i casi in cui si legittima il trattamento dei dati personali senza richiedere il consenso, in ragione del fatto che esso costituisce solo una delle basi giuridiche per il lecito trattamento dei dati personali espres-

⁹¹ La relazione introduttiva alla proposta di Regolamento *e-privacy* considera la normativa sul consenso sovrabbondante, dato che riguarda anche pratiche non lesive della vita privata ma, allo stesso tempo, risulta anche sottodimensionata in quanto non disciplina alcune tecniche di tracciamento, come ad esempio le impronte digitali per accedere ad un dispositivo. Sulla sovrabbondanza dell'informativa cfr. I.A. CAGGIANO, *Il consenso al trattamento dei dati personali*, cit., pp. 19-20, la quale sostiene che gli obiettivi che il legislatore cerca di raggiungere tramite l'informativa, nella pratica si rivelano vani. Infatti, l'utente si pone in un atteggiamento di disinteresse rispetto all'informativa e la percepisce come estranea rispetto all'operazione o al servizio richiesto. Conformemente MISEK, J., *Consent to Personal Data Processing-The Panacea or the Dead End*, in Masaryk UJL & Tech., VIII, 2014, p. 76.

⁹² S. MAZZAMUTO, op. cit., p. 999, ritiene che « la pretesa di elevare la regola del consenso a pietra angolare » non può realizzarsi, dato che vi sono numerose ipotesi in cui lo stesso non è necessario o non è sufficiente. L. GATT, R. MONTANARI e I.A. CAGGIANO, op. cit., pp. 350-351, i quali — sulla base dell'indagine condotta con l'esperimento *Privacy and Internet of Things: a behavioural and legal approach* — evidenziano i limiti del consenso dato che è reso inconsapevolmente e non costituisce un effettivo impedimento alla dannosità del trattamento. Addirittura, la prestazione del consenso potrebbe avere un effetto distorsivo

poiché viene prestato senza che l'utente abbia contezza degli strumenti di tutela *ex post*, essendo convinto che la sola concessione del consenso elimini ogni possibile lesione dei dati personali di cui è titolare. I.A. CAGGIANO, *Il consenso al trattamento dei dati personali*, cit., pp. 20 ss., analizza l'efficacia della normativa, intesa come capacità delle norme giuridiche di raggiungere gli obiettivi prefissati, e l'effettività della tutela, che misura il grado di corrispondenza tra il mezzo di tutela (il consenso) e gli interessi tutelati (la tutela dei dati personali). L'indagine è condotta tramite un'analisi empirica a carattere interdisciplinare nell'ambito del progetto *Privacy and Internet of Things: a behavioural and legal approach* e, sulla base dei risultati ottenuti (esposti nella nota n. 87), l'autrice rileva forti dubbi, sia in merito all'efficacia della normativa, che all'effettività del consenso come tutela *ex ante*, dato che il consenso di regola è prestato irrazionalmente e inconsapevolmente (anche a causa del suo carattere routinario e all'astrattezza del concetto di trattamento dei dati personali e delle sue conseguenze, non facilmente comunicabili all'utente). Tra l'altro, l'autrice conclude con una disamina della tutela *ex post* del risarcimento del danno, evidenziando la sua difficile attuabilità — per l'assenza di un autonomo diritto al risarcimento del danno per illecito trattamento — e la conseguente necessità di fortificare la tutela *ex ante*. Si veda in tal senso anche G. ZANFIR, *Forgetting About Consent. Why The Focus Should Be On "Suitable Safeguards"*, in S. Gu-

samente previste dall'art. 6 GDPR⁹³ e passa in secondo piano rispetto ad altri interessi, come quello della sicurezza⁹⁴. Ne è un esempio l'*eCall*, dispositivo elettronico installato sul veicolo che fornisce un servizio pubblico gratuito in grado di effettuare automaticamente una chiamata di emergenza per allertare i servizi di soccorso in caso di incidente stradale⁹⁵. Anche se i dati sono usati al solo scopo di affrontare le situazioni di emergenza⁹⁶ e la chiamata effettuata fornisce solo le informazioni minime per il soccorso (come il tipo di veicolo, il combustibile utilizzato, l'ora dell'incidente, la posizione esatta e il numero di passeggeri), è molto probabile che si tratti di dati personali, in alcuni casi persino sensibili, per i quali non viene richiesto il consenso da parte del fornitore del servizio *eCall* né dai servizi di pronto intervento, i quali rivestono il ruolo di titolari del trattamento⁹⁷.

Altre evidenti ipotesi in cui viene meno il consenso come base giuridica del trattamento sono quelle — sempre più frequenti — in cui il trattamento sia necessario ai fini dell'esecuzione del contratto di vendita del veicolo o di assicurazione dello stesso⁹⁸, ovvero il trattamento sia obbligatorio per il perseguimento del

TWIRTH, R. LEENES e P. DE HERT (a cura di) *Reloading Data Protection*, 2014, pp. 241 ss..

⁹³ J. MISEK, *op. cit.*, p. 79 ss..

⁹⁴ Ai sensi dell'art. 6, par. 1, lett. d, Reg. 2016/679/UE, il trattamento è lecito — anche senza consenso — qualora sia necessario per la salvaguardia degli interessi vitali (tra cui si può includere la sicurezza) dell'interessato o di un'altra persona fisica.

⁹⁵ Entro il 31 marzo 2018 dovranno essere installati i dispositivi e-call su tutti i nuovi modelli di autoveicoli e l'Europarlamento ha imposto alla Commissione l'obbligo di verificare l'eventuale estensione di tali dispositivi ad altre categorie di veicoli (autobus, camion, pullman, ecc.), nei tre anni successivi al marzo 2018. Regolamento del Parlamento europeo e del Consiglio relativo ai requisiti di omologazione per lo sviluppo del sistema eCall, 29.04.2015, n. 758, in www.eur-lex.europa.eu.

⁹⁶ L'art. 5, par. 2, co. 1, Reg. 2015/758/UE, descrive la tipologia di incidente stradale che comporta l'attivazione del sistema *e-call*.

⁹⁷ Gruppo di lavoro per la protezione dei dati personali, Documento di lavoro sulle implicazioni in materia di protezione dei dati e rispetto della privacy dell'iniziativa *eCall*, 26.09.2006, in www.privacy.it, riteneva che per l'implementazione del servizio *eCall* bisognava valutare in prima battuta se introdurre il servizio come facoltativo o obbligatorio. Nel primo caso era necessario prevedere una soluzione che tenesse conto

dell'autodeterminazione degli utilizzatori di auto, introducendo l'obbligo del consenso dell'interessato e la possibilità tecnica di disattivare/attivare l'*eCall* caso per caso; nella seconda ipotesi era necessario prevedere una normativa specifica che tenesse conto della protezione dei dati personali. Ai sensi dell'art. 4, Reg. 2015/758/UE, il sistema è attualmente obbligatorio e, quindi, non è richiesto il consenso. Allo stesso tempo, però, bisogna sottolineare che i dati non saranno comunicati a terzi senza il consenso dell'interessato e dettagliate norme tecniche (tra cui la c.d. *privacy by design*) consentiranno di evitare lo scambio di dati personali tra il sistema di bordo *eCall* e soggetti terzi. Peraltro, 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. Tra l'altro, i costruttori garantiscono che il sistema *eCall* non sia tracciabile né oggetto di controllo costante e che i dati siano automaticamente e costantemente cancellati dalla memoria interna (art. 6, Reg. 2015/758/UE).

⁹⁸ Art. 6, lett. b, GDPR. Ciò si verifica in tutte le ipotesi in cui nel contratto di vendita ci sia una clausola che obblighi il produttore a monitorare il funzionamento del veicolo, in qualità di titolare del trattamento. Allo stesso modo, nel contratto di assicurazione, l'assicurazione (titolare del trattamento) potrebbe monitorare l'anda-

legittimo interesse del titolare del trattamento a non incorrere in responsabilità da prodotto difettoso ⁹⁹.

Appare, pertanto, quantomeno dubbia la funzionalità dello strumento del consenso dell'interessato per la tutela della sfera personale ¹⁰⁰ e sembrerebbe preferibile rafforzare altre forme di tutela *ex ante*, prima tra tutti la c.d. *data protection by design*.

7. LA *DATA PROTECTION BY DESIGN* COME PARTICOLARE STRUMENTO PER IL RAFFORZAMENTO DELLA TUTELA PREVENTIVA DEI DATI PERSONALI.

Come si è tentato di argomentare nei paragrafi precedenti, dall'analisi dei dati intercambiati dai veicoli connessi è possibile elaborare dettagliati profili dei soggetti a bordo, i quali non sempre sono stati opportunamente informati circa il trattamento dei propri dati personali né della possibile profilazione.

Ipotizzando il superamento, anche solo parzialmente, del consenso dell'interessato quale requisito necessario per il lecito trattamento dei dati personali, una valida alternativa per garantire in concreto la liceità del trattamento potrebbe essere rappresentata dal rafforzamento del principio della c.d. *data protection by design*, oltre a quello della c.d. *data protection by default* (art. 25, GDPR) ¹⁰¹.

mento di guida del conducente, se espressamente previsto nel contratto di assicurazione, per individuare più facilmente il soggetto responsabile in caso di incidente automobilistico. Tale fattispecie è sempre più comune a seguito dell'introduzione del sistema di scatola nera che, appunto, raccoglie i dati relativi all'andamento dell'autovettura. Infatti, l'adozione della scatola nera viene caldeggiata dalle compagnie assicurative come misura di contrasto delle frodi e, di conseguenza, come strumento per abbassare i prezzi delle polizze RC Auto.

⁹⁹ Ai sensi dell'art. 6, lett. f, GDPR, il produttore (titolare del trattamento) ha legittimo interesse ad adempiere agli obblighi inerenti la sicurezza dei prodotti — come quello imposto dall'art. 5, par. 1, sub. 4, lett. b, Dir. 2001/95/CE, avente a oggetto i controlli a campione sui prodotti commercializzati — onde evitare di essere ritenuto responsabile a causa di un malfunzionamento del prodotto.

¹⁰⁰ S. MAZZAMUTO, *op. cit.*, p. 998, ritiene che il problema non sia quello di una tutela dei dati personali di tipo proprietario, quanto quello di prendere atto che i dati personali inevitabilmente circolano e, di conseguenza, occorre predisporre regole che garantiscano all'interessato un continuo monitoraggio e un potere di controllo sui

dati e sulla loro circolazione. E. ROPPO, *Informatica e tutela della privacy e diritti di libertà*, in G. ALPA (a cura di), *Computers e responsabilità civile*, Milano, 1985, p. 23, aveva già evidenziato che al giorno d'oggi la tutela della *privacy* non è una tutela di tipo proprietario, bensì di tipo procedimentale fondata sulla necessità di canalizzare le inevitabili attività di raccolta e utilizzo delle informazioni ed evitare usi impropri dei dati, grazie alla predisposizione di appositi controlli. DI MAJO A., *Il trattamento dei dati personali tra diritto sostanziale e modelli di tutela*, in V. CUFFARO, V. RICCIUTO, V. ZENO-ZENCOVICH (a cura di), *Trattamento dei dati e tutela della persona*, Milano, 1998, p. 233 ss. esclude che il modello di tutela dei dati personali possa essere di tipo dominicale e/o proprietario. I.A. CAGGIANO, *Il consenso al trattamento dei dati personali, cit.*, pp. 30 ss., ipotizza un sistema nel quale si supera il generale requisito del consenso per il trattamento dei dati personali, ma configura comunque un potere di controllo dell'interessato, seppur limitatamente ai suoi dati sensibili.

¹⁰¹ Nella relazione introduttiva alla proposta di Regolamento *e-privacy* viene ripresa la consultazione pubblica condotta dalla Commissione europea dal 12 aprile al 5 luglio 2016, in merito alla questione del

Il principio della protezione dei dati personali fin dalla progettazione (c.d. *data protection by design*) è un chiaro esempio di tecno-regolamentazione¹⁰²: fin dalla fase in cui vengono progettati i prodotti e i servizi — oltre che nell'esecuzione del trattamento — il titolare deve utilizzare la tecnologia per garantire soluzioni che tutelino la *privacy* e la sicurezza degli utenti¹⁰³. Un'altra ipotesi di tecno-regolamentazione è il principio della c.d. *data protection by default*, la quale richiede l'utilizzo di misure tecniche e organizzative che consentano un approccio più selettivo al fine di evitare di catturare un'eccessiva quantità di dati, limitandosi solo ai dati necessari¹⁰⁴ per migliorare la prestazione

consenso ai marcatori. Ben l'81,2% dei cittadini e il 63% delle autorità pubbliche si sono dichiarati favorevoli all'imposizione di obblighi ai fabbricanti di apparecchiature terminali affinché commercializzino prodotti con impostazioni di vita privata attive preimpostate; il 58,3% del settore, invece, appoggia l'opzione di autoregolamentazione o coregolamentazione.

¹⁰² L'idea di utilizzare le tecnologie per disciplinare la tecnologia stessa e, in particolar modo, gli aspetti concernenti la tutela dei dati personali, risale all'art. 17 della Dir. 95/46/CE, attraverso l'introduzione delle misure tecniche e organizzative che il responsabile del trattamento doveva attuare per tutelare i dati personali. Proprio in quegli anni, infatti, si sviluppano le *Privacy Enhancing Technologies* (PET), ossia tutte quelle tecnologie nell'ambito dell'*Information and Communications Technology* (ICT) che hanno lo scopo di aumentare la protezione dei dati personali. Le PETs si dividono in: *subject-oriented PETs* che limitano la riconoscibilità di un individuo da parte di terzi, *object-oriented PETs* che proteggono l'identità personale, *transaction-oriented PETs* che tutelano i dati relativi alle transazioni e, infine, *system-oriented PETs* che creano delle zone di interazione all'interno delle quali i soggetti non sono riconoscibili, la loro identità è nascosta e i dati sulle transazioni non vengono memorizzati. Il termine *privacy by design*, invece, già presente negli Stati Uniti e in Canada, è stato coniato nel 2010 da Ann Cavoukian, Privacy Commissioner dell'Ontario, nel corso della 32^a Conferenza mondiale dei Garanti *privacy*. Cfr. G. PASCUZZI, *op. cit.*, pp. 79 ss.; 32^{ma} Conferenza internazionale delle autorità di protezione dei dati, Gerusalemme, 27-29 ottobre 2010, in www.icdpc.org. La *privacy by design* non può essere propriamente collocata all'interno delle PETs dato che queste sono tecnologie volte a tutelare la *privacy* degli utenti mentre la

privacy by design è un principio giuridico (espressamente disciplinato) il quale prevede che le tecnologie devono essere utilizzate per tutelare la *privacy* già nella fase di progettazione e, successivamente, durante il trattamento. R. D'ORAZIO, *op. cit.*, pp. 102-103.

¹⁰³ R. D'ORAZIO, *op. cit.*, pp. 81 ss., puntualizza che il principio della *privacy by design* non può essere applicato in via assoluta e incondizionata, ma deve tenere conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito applicativo, del contesto e delle finalità del trattamento, come espressamente dispone il dato normativo (art. 25, par. 1, Reg. 2016/679/UE). In conseguenza di ciò, sono ipotizzabili casi in cui il principio non potrebbe concretamente essere messo in pratica. Allo stesso tempo, però, il titolare del trattamento è tenuto ad adottare misure tecniche e organizzative per garantire e dimostrare che il trattamento è posto in essere nel rispetto del GDPR (art. 24, par. 1, Reg. 2016/679/UE), comportando un'inversione dell'onere della prova in capo a quest'ultimo, il quale dovrà provare la conformità del trattamento rispetto al nuovo Regolamento UE (dettagliatamente, dovrà provare di aver adottato tutte le precauzioni necessarie per garantire la conformità al Regolamento UE fin dall'inizio, quando è stato progettato il prodotto o servizio, e di aver raggiunto la conclusione che i dati personali siano adeguatamente protetti). Ciò implica che il titolare deve prestare molta attenzione nell'attuazione del principio della *privacy by design*, onde evitare di incorrere in sanzioni di cui agli artt. 83 e 84, GDPR.

¹⁰⁴ L'art. 3 cod. *privacy* prevede il c.d. principio di necessità del trattamento dei dati, che si applica ai sistemi informativi e, prime tra tutti, alle ICT. Pertanto, queste devono essere predisposte in modo da assicurare che i dati personali e i dati identificativi siano trattati solo nei casi necessari,

dei servizi e la sicurezza dei prodotti, nonché per comprendere le richieste del mercato (*market analysis*).

Nell'ambito della *data protection by design* si è già discusso della pseudonimizzazione come bilanciamento al processo di profilazione dell'utente (v. *supra* par. III). Si rammenta che i dati pseudonimizzati non possono essere equiparati a quelli anonimi, in considerazione del fatto che i primi continuano a permettere l'identificazione delle singole persone e le rendono trasversalmente collegabili a diversi insiemi di dati¹⁰⁵. Tuttavia, nell'ambito della disciplina normativa sulla tutela dei dati personali — in cui l'anonimizzazione non rientra — la pseudonimizzazione risulta essere un adeguato strumento di tutela *ex ante*, seppur con delle eccezioni¹⁰⁶. Concretamente, esempi tipici di pseudonimizzazione sono la crittografia con chiave segreta, la funzione di *hash* (e le sue varianti) nonché la tokenizzazione¹⁰⁷.

Aumentando la protezione dei dati personali sin dalla fase di progettazione, anche grazie all'ausilio dei meccanismi sopraesposti — si potrebbe ottenere un'effettiva tutela preventiva dei dati personali degli interessati del trattamento, senza la necessità di ricorrere (in tutto o in parte) al macchinoso strumento del consenso¹⁰⁸. Per ottenere concretamente tale risultato è opportuno che i giuristi lavorino in sinergia con gli ingegneri e gli informatici nei *team* di sviluppo dei sistemi di guida autonoma — e delle nuove tecnologie in generale — in modo da completarsi vicendevolmente.

cioè quando per il raggiungimento delle finalità consentite non possano essere utilizzati dati anonimi o caratterizzati da una limitata identificazione degli utenti. Le ICT devono essere progettate in modo da minimizzare le quantità dei dati personali che devono essere processati e il principio di minimizzazione è espressamente previsto nel GDPR all'art. 5, par. I, lett. c, e richiamato nell'art. 25 a proposito della *data protection by design*. SANTOSUOSSO A., *Diritto, scienza e nuove tecnologie*, 2^a ed., Milano, 2016, p. 307. La *ratio* del principio di minimizzazione è quella di ridurre il numero di dati trattati aumentando così le tutele, ma è anche quella di semplificare gli adempimenti da porre in essere, sulla stessa scia del principio di necessità. In tal senso R. D'ORAZIO, *op. cit.*, p. 97.

¹⁰⁵ Parere del Gruppo di lavoro n.4/2014, *cit.*, p.11.

¹⁰⁶ Y.A. DE MONTJOYE, C. HIDALGO, M. VERLEYSEN e V. BLONDEL, *Unique in the Crowd: The privacy bounds of human mobility*, in *Nature*, n. 1376, 2013. Team di ricercatori del Massachusetts Institute of

Technology (MIT) hanno analizzato un insieme di dati pseudonimizzato, composto da 15 mesi di coordinate di mobilità spaziotemporale di 1,5 milioni di persone in un territorio compreso in un raggio di 100 km. I risultati dell'analisi hanno dimostrato che, nonostante le identità delle persone fossero state pseudonimizzate sostituendo i dati personali identificativi con altre etichette, il 95% delle persone poteva essere identificato mediante quattro luoghi e che bastavano due luoghi per identificare più del 50% delle persone interessate (tra l'altro, almeno uno di tali luoghi è facilmente immaginabile, coincidendo molto probabilmente con l'abitazione o con il luogo di lavoro).

¹⁰⁷ Parere del Gruppo di lavoro n.4/2014, *cit.*, pp. 21 ss..

¹⁰⁸ R. D'ORAZIO, *op. cit.*, p. 88, esalta le possibilità offerte dalla *privacy by design* e *by default*, che risultano propizie per la convergenza tra le regole europee e quelle di pesi terzi al fine di creare un quadro uniforme di norme operazionali che costituisca un punto di riferimento generale per tutte le attività di trattamento dei dati personali.

Abstract

Autonomous vehicles are already on the market. As well as driving us, they will store and process large amounts of personal information. Users will be unaware of this, and the risks it generates. This information is personal data, and so is regulated by Reg. 679/2016/EU, commonly known as General Data Protection Regulation (GDPR). But is this European legislation sufficient to offer the necessary protection to users of self-driving cars? In particular, an important question is whether consent to the processing of personal data is really functional to achieve the objectives set out in the GDPR or whether further protection is required.