www.jusletter-it.eu

Maria Cristina Gaeta

The Issue of Data Protection in the Internet of Things with Particular Regard to Self-driving Cars

Category: Articles
Region: Italy
Field of law: AI & Law; Electro Mobility; Data Protection

Citation: Maria Cristina Gaeta, The Issue of Data Protection in the Internet of Things with Particular Regard to Self-driving Cars, in: Jusletter IT 23 November 2017

ISSN 1664-848X, https://jusletter-it.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77 EDITIONS WEBLAW

Contents

1. An Introduction on Internet of Things and Self-driving Cars

[Rz 1] Nowadays the pervasiveness of the Internet is undeniable. It affects the private and working life of every human being, who is constantly monitored through the growing number of identification and tracking technologies. At the same time, though, people cannot do without these technologies because they improve the services offered, which are extremely useful (perhaps essential) for most of the daily activities.

[Rz 2] Internet development has been greatly enhanced by the extension of this network to the world of objects, a phenomenon known as the Internet of Things (IoT). In particular, it is an evolution of the Internet network, thanks to which the objects interact with each other, through sensors and without human intervention, exchanging data and accessing information stored in databases.[1] This information architecture has been defined as a network which connects physical or virtual objects that become recognizable and acquire intelligence through the ability to communicate data about oneself and about the environment around them.[2] For this reason, such objects are defined as intelligent objects. They are tagged with a radio frequency identification tag with a single ID called Electronic Product Code (EPC).[3] Currently included in this category are incredibly disparate kinds of objects – traffic lights, cars, thermostats, refrigerators, alarm clocks, watches, surveillance cameras and many others. There are so many smart things that the concept has moved from «Internet of Things» to «Internet of everything». In addition, connectivity is growing steadily and it is expected that by 2020 more than 20 million objects will be connected to each other.[4]

[1] Alberto Maria Gambino, Informatica giuridica e diritto dell'informatica, Treccani Diritto online (2013), http://www.treccani.it/enciclopedia/informatica-giuridica-e-diritto-dell-informatica_%28Diritto-on-line%29/ (all websites last accessed on 24 October 2017).

[2] European Research Cluster on the Internet of Things (IERC), Internet of Things Strategic Research Roadmap (2nd edition 2011), p. 10, http://www.internet-of-things-research.eu/pdf/IoT_Cluster_Strategic_Research_Agenda_2011.pdf.

[3] About Radio Frequency Identification (RFID) see Erica Caterina Pallone, «Internet of Things» e l'importanza del diritto alla privacy tra opportunità e rischi (2016), vol. 17, 55 Ciberspazio e diritto, p. 174 f. About Internet of Things definition see Rolf H. Weber, Internet of things: new security and privacy challenges (2010), Computer Law and Security Review, 26(1), p. 23 f. Finally, with regard to the introduction of the term Internet of Things Kevin Ashton, That «Internet of Things» Thing. In the real world, things matter more than ideas (2009), RFID Journal, p. 1, http://www.rfidjournal.com/articles/view?4986; Stephan Haller/Stamatis Karnouskos/Christoph Schiroh, The Internet of Things in an Enterprise Context (2008), Future Internet – FIS 2008, p. 14 f..

[4] Mark Hung/Gartner (ed.), Leading the IoT – Gartner Insights on How to Lead in a Connected World (2017), p. 13, http://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf; Eric Hannon/Colin McKerracher/Itamar Orlandi/Surya Ramkumar, An integrated perspective on the future of mobility (2016), p. 1 ff., https://www.mckinsey.com/business-functions/sustainability-and-resource-productivity/our-insights/an-integrated-perspective-on-the-future-of-mobility.

[Rz 3] In this area, one of the most advanced businesses is undoubtedly the car industry. Indeed, by the end of the first twenty years of our century, there will be about 250 million vehicles connected online[5] and the automotive market will grow exponentially, up to quadruple.[6] Moreover, around 2025, there will be such a level of automation that the driver will not have to constantly monitor the vehicle, even if he has to be able to resume control at all times.

[Rz 4] To communicate with each other, the new vehicles must be connected online, and as a result of this connection the automotive industry too is included in the Internet of Things network. Autonomous vehicles are often defined as connected vehicles to emphasize their ability to connect to the network. There are essentially three types of vehicle connections. The first and most common type of communication is between automated vehicles and different categories of devices (e.g. smartphones, smart watches, tablets and personal computers) known as the Vehicle to Device Communications (V2D). Secondly, there is Vehicle to Infrastructure Communications (V2I), a more specific type of communication between vehicles and infrastructures (such as road traffic lights or speed cameras). Finally, the most sophisticated type of communication is Vehicle to Vehicle Communications (V2V), as it presupposes fully autonomous driving, or at least a high level of automation.[7]

[Rz 5] The level of the vehicle communication is directly proportional to the level of automation of the vehicles[8], even though connectivity is just one of the requisites needed to achieve complete automation of vehicles.

[Rz 6] Thanks to the development of autonomous and connected driving, mobility is evolving more and more rapidly. A significant number of possible societal benefits has been identified, including improvement of road traffic conditions, reduction of environmental pollution, development of the sharing economy, increased transport safety and the extension of mobility to people who are usually excluded (e.g. children, elderly and disabled) by transforming mobility into a genuine service (so-called «mobility as a service»).[9] The IoT is undoubtedly the most important innovation in the field of Information Technology (IT). However, in addition to the many advantages, there are a number of issues still to be resolved and the automotive sector is one that most urgently requires regulation.[10] Among the key issues are how to allocate liability in case of road accidents caused by driverless cars malfunctioning, a topic that has already been explored in depth elsewhere.[11] Instead, in the light of the European reform of the protection of personal

[5] Gartner Estimates, Press Release «Gartner Says By 2020, a Quarter Billion Connected Vehicles Will Enable New In-Vehicle Services and Automated Driving Capabilities» (2015), https://www.gartner.com/newsroom/id/2970017; James Manyika/Michael Chui/Jacques Bughin/Richard Dobbs/Peter Bisson/Alex Marrs, Disruptive technologies: Advances that will transform life, business, and the global economy (2013), https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/disruptive-technologies.

[6] Richard Viereckl/Jörg Assmann/Christian Radüge, In the fast lane: The bright future of connected cars (2014), p. 5, https://www.strategyand.pwc.com/reports/in-the-fast-lane.

[7] Para. 2 lit. d. Declaration of Amsterdam of 14 and 15 April 2016 on Cooperation in the field of connected and automated driving.

[8] Automation degrees have been classified by multiple authors and research centres. More precisely see: Tom M. Gasser/Daniel Westhoff, Definitions of Automation and Legal Issues in Germany (2012), workshop of German Federal Highway Research.

[9] Introduction of Declaration of Amsterdam (note 7).

[10] European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics, (2015/2103(INL)) nos. 24 ff.

[11] Maria Cristina Gaeta, Automazione e responsabilità civile automobilistica (2016), 5, Responsabilità civile e previdenza, p. 1718 ff.

data,[12] this paper will focus on the issue concerning the protection of personal data processed by autonomous vehicles and the related profiling process of the user, who uses such technologies daily and is often unaware of the risks.

[Rz 7] In the field of data protection, the consent to the processing of personal data in self-driving cars involves several issues, which lead to wonder if consent is still an appropriate regulatory tool for the protection of personal data. Indeed, the consent model just does not work without causing risk to the driver or passengers on board, and asking for it is too impractical. For example, if a driver is driving with 100 km/h on the motorway, the last thing he wants is a popup of a consent form – that would be very dangerous. Under the current level of automation (level 3),[13] the driver has to be able to resume the control of the vehicle in case of emergency. In a case like this it is a safety problem to be having to give consent all the time.

[Rz 8] Furthermore, in particular in the V2I and V2V communication, some of the data have to be exchanged in split seconds and the user could not have time to give his or her consent to the processing of personal data. Making some examples: when a driver drives into an area with congestion charge, the city infrastructure has to determine if he paid the charge and let him in; on the motorway a self-driving car tells incoming autonomous vehicles the characteristics of the self-driving cars and how the driver is driving, to allow another vehicle to anticipate its behaviour. In these situations, even if the driver could find the time to think about this it would be too late once a decision is made.

[Rz 9] Finally, the driver is not the only person whose data is collected. Data is also collected about passengers, and also potential third parties outside the vehicle, captured by self-driving car communication while driving. It is obvious that the consent model does not work here and that some processing of personal data is necessary.

[Rz 10] For this reason, as will be attempted to demonstrate below, we need sector specific laws for robotics, and – in particular – sector specific regulations for self-driving cars. The difference between robotics applications are too significant to allow for a single «law of robotics».

2. Data Protection in Self-driving Cars

2.1. The Exchange of Personal Data between Connected Vehicles

[Rz 11] The protection of personal data is a matter that has always affected society, re-emerging from time to time in different aspects. In current parlance the terms confidentiality, privacy and data protection are often used as synonyms. While connected, these three are nonetheless different concepts. Confidentiality can be divided into two aspects: (i) the right to *privacy*

[12] On May 4, 2016, they were published in the Official Journal of the European Union (OJ): Regulation 679/2016/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/1, well know as General Data Protection Regulation (GDPR); Directive 2016/680/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89; Directive 2016/681/EU of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime [2016] OJ L119/132.

[13] *See* above, note 8.

(more precisely the respect of private life) and (ii) the protection of personal data, as fundamental freedom,[14] and as an autonomous personality right which is found in the power of self-determination.[15] This distinction is also clearly reflected in Art. 7 and 8 at the Charter of Fundamental Rights of the European Union. However, data protection, even if it constitutes an autonomous personality right, could be considered as a subcategory of the right to privacy, since one of the cases in which the right to privacy is infringed is the abusive treatment of personal data. The aim of this paper is to analyse the protection of personal data, with particular regards to some aspects closely relating to the development of autonomous vehicles.

[Rz 12] The cross-strait impact of the Internet and related especially of the IoT on human life has attracted the attention of several European authorities. In particular, the Article 29 Data Protection Working Party (Article 29 WP) [16] adopted an opinion in 2014 aimed at finding solutions that enforce privacy protection rules also in the Internet of Things.[17] Based on a typical law and economics approach, the Article 29 WP compared citizens' interests in the protection of their personal data and those of companies operating in this sector, who receive significant economic benefits from the spread of IoT, trying to dictate guidelines to extend the existing European legislation on data protection to smart things as well.

[Rz 13] In order to define and analyse the IoT phenomenon, the Global Privacy Enforcement Network (GPEN)[18] has launched Privacy Sweep 2016. It is an international survey to verify respect for privacy and data protection in the Internet of Things field – strengthening cooperation between the Data Protection Authorities of the 26 countries of the world who have joined the initiative[19]. The investigation ended on September 22, 2016 with worrying results. In fact, more than 60% of smart things have not passed the GPEN test.

[Rz 14] With regard to self-driving cars, it is clear that the connectivity of these vehicles results in the collection, processing, and transfer of personal data,[20] such as vehicle and user's localisation, routes or personal data coming from the synchronization of the user's mobile phone with the connected car. More precisely, manufacturers collect data not only on the performance of their products (which also makes it possible to quickly detect a malfunction and determine liability in case of a car accident) but also users' personal information, who are often unaware of this

[14] Giuseppe Francesco 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 (2015), 2, Osservatorio del diritto civile e commerciale, p. 16 ff.

[15] Cesare Massimo Bianca/Francesco Donato Busnelli (eds.), La protezione dei dati personali, vol 1 (CEDAM 2007), p. XX ff.; Cesare Massimo Bianca, Diritto civile, vol. I, La norma giuridica. I soggetti, (2nd edition, Giuffrè, 2002), p. 180. The difference between the right to privacy and data protection is evident in the Charter of 18 December 2000 of Fundamental Rights of the European Union [2000] OJ C 364/1, art. 7–8. However, the right to privacy may be infringed in a number of cases, including the one of the unlawful processing of personal data. For this reason, the right data protection is a specification of the right to privacy, even if it constitutes an autonomous personality right.

[16] The Article 29 Data Protection Working Party (Art. 29 WP) was established by art. 29 Directive 95/46/CE.

[17] Art. 29 WP, Opinion 8/2014 of 16 September 2014 on the on Recent Developments on the Internet of Things (2014), p. 10 ff., which refers to wearable computing, quantified self and domotics, but appears to be applicable to any area of IoT.

[18] In 2007, the Council of the Organisation for Economic Co-operation and Development (OECD) adopted the Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy. The Recommendation imposed the goal of creating an informal network of Personal Data Protection Authorities on OECD member states, from which the Global Privacy Enforcement Network was born.

[19] For more details on Privacy Sweep 2016, included results are available on www.privacyenforcement.net.

[20] Alexandra Wood/David R. O'Brien/Urs Gasser, Privacy and Open Data Research Briefing (2016), Networked Policy Series, Berkman Klein Center Research Publication No. 2016-16, p. 4.

processing of their personal data.[21] In addition, this data may be intercepted by third parties who use or sell it for diverse purposes.

[Rz 15] Research commissioned by the *Fédération Internationale de l'Automobile* (FIA), focusing on the flow of data exchanged between cars and their respective manufacturers, revealed the quantity and quality of data that last-generation vehicles are able to exchange[22]. Additionally, based on the results of this research, FAI launched the My Car My Data project[23] to raise awareness about the processing of personal data and the need to introduce specific legislation.

[Rz 16] It is therefore appropriate to ask whether the use of privacy statements is adequate and whether the consent to the processing of personal data[24] is a functional tool for the protection of personal data.[25] For personal data, consent constitutes a lawful basis for processing (art. 7 of the General Data Protection Regulation [GDPR]). For personal data that in addition falls into one of the categories listed in art. 9 GDPR (i.e. sensitive data), consent is an exception to the general prohibition of processing data of that kind.

[Rz 17] The issue that is being addressed in this paper results from the fast development of technology that makes it difficult to provide rational and conscious consent. In such cases it is appropriate to ask: «Is there a real self-determination right for the user? Is consent really provided in compliance with the current legislation? Is consent still an appropriate regulatory tool for the protection of personal data?»[26]

2.2. The Possible Integration between Profiling and Pseudonymisation Processes

[Rz 18] User consent has a particular function in relation to the profiling process. This term refers to any form of automated processing of different types of personal data related to a very high number of subjects through specific algorithms. The purpose of the profiling is to create a detailed profile of a data subject. Expressly, profiling aims to evaluate certain personal aspects of a natural person, such as professional performance, economic situation, health, preferences, interests, behaviour, localisation or movement.[27] This creates a user's digital profile, which is kind of additional individual representation, different from (a) personal identity, that is some, the set of characteristics that identify the individual, and from (b) digital identity, that is the projection of a real individual in the digital world.

[21] Alessandro Montelero, Data Protection, E-Ticketing, and Intelligent Systems for Public Transport (2015), International Data Privacy Law 2015:5(4), p. 309 ff., https://ssrn.com/abstract=2659732.

[22] Fédération Internationale de l'Automobile, FIA Reveals what Data is being Tracked and how the Public Reacts to Connected Cars (2015), https://www.fia.com/news/fia-reveals-what-data-being-tracked-and-how-public-reacts-connected-cars.

[23] MyCar My Data Project Website, www.mycarmydata.com.

[24] Art. 4 para. 1 n. 11 GDPR defines consent of the processing of personal data.

[25] W. Kuan Hon/Christopher Millard/Jatinder Singh, Twenty Legal Considerations for Clouds of Things (2016), Queen Mary University of London, School of Law, Legal Studies Research paper no. 216/2016, p. 21 ff., https://ssrn.com/abstract=2716966.

[26] *Ibid.*, p. 5 ff.

[27] At the international level, the Strasbourg Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, no. 108, ensured the respect of the right to private life, with regards to the automated processing of the data subject's personal data.

[Rz 19] The automated profiling process is defined by art. 4 para. 1 n. 4, and regulated by art. 22 GDPR. The EU Regulation provides the prohibition of automated profiling as a general principle, unless: (a) this is necessary for entering into, or performance of, a contract, (b) it is authorised by European Union or Member State law to which the controller is subject or (c) (this is the hypothesis which we intend to emphasise) it is based on the data subject's explicit consent.[28] As to this last option, on one hand, profiling is initially begun with user's consent, which often does not represent a free and conscious manifestation of his or her will. On the other hand, there are some cases in which it is possible to profile a data subject without his or her explicit consent when it is the result of an algorithmic process of personal data (e.g. profiling), and the user had provided the consent for each single process.[29]

[Rz 20] In this regard, it is of extreme importance to protect the right to object of the data subject at any time of the processing of his or her personal data, which is based on automated decision making, including profiling (art. 21 GDPR). This protection is flanked by the right to be informed about the existence of automated decision-making processes by the data controller, including profiling and, at least in those situations, to receive information about the logic involved, as well as the significance and the consequences of such processing for the data subject (art. 13 para. 2 lit. f. and art. 14 para. 2 lit. g GDPR).[30] Finally, given the risk to the rights and freedoms of the data subject, before the processing the controller shall carry out an assessment of the impact of the processing operations on the protection of personal data, especially when it is a profiling process (art. 35 para. 2 GDPR).

[Rz 21] Personal data allows the creation of detailed user profiles based, for example, on behaviour, habits, health, age, and sexual, political, or religious orientation. This produces a particularly invasive monitoring of private life, which could erode individual freedoms. At the same time, however, profiling is very important for market analysis, as manufacturers can accurately identify which products are most sought after and in what quantities, and could also improve them and reduce their risk. Therefore, it is necessary to find the right balance between user profiling and the protection of his or her personal data, with particular regard to the profiling process. In this sense, the GDPR expressly defines pseudonymisation (art. 4 para. 1 n. 5 GDPR), which is a process of irreversible dissociation of personal data from the data subject, so that the data can no longer be attributed to a subject identified or identifiable without the use of additional information that is kept separately and is protected by specific technical and organizational measures to achieve and maintain the dissociation.

[Rz 22] Pseudonymisation is a process different from anonymisation (regulated under art. 12 Directive 2016/681/EU as depersonalisation), even from the point of view of the protections granted. Data is anonymised through masking the information which could serve to directly identify the data subject to whom the data relate. For pseudonymised data, there is the possibility to identify the data subject by accessing separately stored information. For this reason, only pseud-

[28] Dimitra Kamarinou/Christopher Millard/Jatinder Singh, Machine Learning with Personal Data (2016), Queen Mary University of London, School of Law, Legal Studies Research paper no. 247/2016, p. 14 ff., https://ssrn.com/abstract=2865811.

[29] Ilaria Amelia Caggiano, Il consenso al trattamento dei dati personali (2017), p. 3 ff., https://www.dimt.it/index.php/it/la-rivista/16175-il-consenso-al-trattamento-dei-dati-personali-tra-nuovo-regolamento-europeo-gdpr-e-analisi-comportamentale-iniziali-spunti-di-riflessione.

[30] See also recitals 60, 63 and 71 GDPR.

onymised, and not anonymised data, is subject to the regulation in the GDPR.[31] Given these premises, it should be pointed out that in practice, it is not possible to exclude the possibility of identifying the data subject in absolute terms, even when the personal data is anonymous, given that the current techniques of analysis, combination, and comparison of information identify the user.[32]

[Rz 23] The tendency towards pseudonymisation as a possible solution to the profiling of an identified or identifiable user has long been supported considering that the profiling process can also be performed without identifying profiled subjects. Therefore, different types of users are actually profiled without being able to individually identify each single profile processed, as pseudo-anonymous.[33] In fact, even non-identifying data may give a somewhat exhaustive description of a user or group of subjects (i.e. clustering), achieving the purpose (or closely do so) pursued by profiling but without damage to the interests of the subjects from which the data comes. With respect to the use of pseudonymisation process as a possible solution, the recital 29 of the GDPR states that pseudonymisation should also be encouraged in relation to big data in order to process large amounts of data without infringing the right to data protection. To ensure this protection, the GDPR imposes specific conditions about big data analysis: the use of appropriate technical and organizational measures (such as data protection by design and data protection by default) and of security measures to ensure that the additional information needed for identification is kept separately from the pseudonymised data.

3. The Need for a Framework of Rules for the Protection of Personal Data Exchanged by Connected Vehicles

[Rz 24] The European initiatives for introducing a regulatory framework on Robotics are numerous. Recently, with the Resolution of 16 February 2017, the European Parliament recommend to the European Commission to submit a bill on civil law rules on robotics and artificial intelligence (AI) and non-legislative acts (such as guidelines and codes of ethical conduct). The purpose of the European Parliament resolution is to address the main issues foreseeable in the next 10–15 years, taking into account the Charter on Robotics attached to the Resolution.[34] In addition, the European Parliament considers that the automotive sector is in most urgent need of efficient European Union and global rules, in order to ensure the cross-border development of self-driving cars, the exploitation of their economic potential and the benefits from the technology.[35] Also, in the Declaration of Amsterdam of 14 and 15 April 2016 on Cooperation in the field of connected

[31] Recital 26 GDPR; Art. 29 WP, Opinion 8/2014 (note 17), p. 10 ff.

[32] Art. 29 WP, Opinion 5/2014 of 10 April 2014 on Anonymisation Techniques (2014), considers that it is difficult to create anonymous data while retaining all the information needed to carry out the required activities.

[33] For completeness, it should be noted that pseudonymisation is only one of the possible measures of protecting of personal data which concretizes the principle of data protection by design, and it is possible to foresee others, as expressly provided by recital 28 GDPR.

[34] European Parliament resolution on Civil Law Rules on Robotics (note 10), n. 51.

[35] *Ibid.*, n. 25. About the international regulation, in order to allow automated driving, the European Parliament considers it appropriate to amend the Vienna Convention on Road Traffic of 8 November 1968, and in particular art. 8 and 13, which require a driver on board of the vehicle, who has to monitor the vehicle and keep control on it, see Ivi, n. 60 ff.

and automated driving,[36] the need to develop and maintain a joint program with other European countries has been underlined to support these goals, and to remedy the problems arising from the development of this new type of driving.

[Rz 25] Regarding the protection of personal data, as a specific aspect to be regulated with reference to robotics, the GDPR came into force on 24 May 2016. The EU Regulation will be applicable to all EU Member States from 25 May 2018, and the legislation of each Member State will have to be adjusted to accommodate the GDPR (art. 99 GDPR). The European Resolution points to the centrality of the issue of data protection and the EU Parliament is clear in establishing that civil law rules on robotics have to be compliant with the GDPR, art. 7 and 8 of the Charter of Fundamental Rights of the European Union, and art. 16 of the Treaty on the Functioning of the European Union (TFEU), although other aspects of data protection have to be addressed with particular regard to robotics. In addition, the EU Resolution asks the Commission to ensure the respect of the principles of data protection by default and by design (e.g. pseudonymisation), to implement data protection principles such as data minimisation.[37]

[Rz 26] On this basis, it is evident that there is a strong need to introduce European (or even better global) legislation that regulates autonomous vehicles in accordance with existing rules, which are not entirely adequate.[38] In this way, the first question to be answered is whether it is sufficient to introduce robotics regulations in general or whether it is more appropriate to provide an *ad hoc* discipline for the main sectors of robotics, including, of course, the one of autonomous vehicles.[39] The second solution seems preferable, as well as in line with the EU Resolution. The fields of robotics are so numerous and different that generic legislation would risk to miss all the specific issues of this particular field. This need of specific regulations is even more evident in the transition phase in which we are, which is based on partial automation. As a matter of fact, until total automation is achieved, the differences between the types of robots will be obvious. For example, self-driving cars are different from drones and, until both reach a high level of automation, they will be characterized by a substantial distinction: the first are directly piloted, the second ones are remotely pilot devices. Furthermore, autonomous vehicles are also different from cleaning robots or toy robots. They are inherently dangerous environments for their owners, and therefore a specific and detailed regulation is sensible – in particular because a mistake could put the driver, passengers or third parties at risk.

[Rz 27] Numerous States that have begun to consider specific legislation for self-driving cars. In the US, the National Highway Transportation Safety Administration (NHTSA) has recognized the Self Driving System (SDS) as a driver of the vehicle and in this way extended the road safety regulations, updating the Federal Register.[40] In Europe, Germany was the first and only nation

[36] Declaration of Amsterdam (note 7).

[37] European Parliament resolution on Civil Law Rules on Robotics (note 10), n. 19 ff.

[38] Weber (note 3), p. 26 ff.; IERC (note 2).

[39] The term robot derives from the Czech word robot, which literally means work (forced) and was used for the first time by Karel apek in Rossum's Universal Robots (RUR) (1920), which refers to the automation working instead of workers. Nowadays, the traditional idea of robots, according to which it is a machine with humanlike appearances, is overcome, so that even autonomous vehicles are included in the category of robots. The European Parliament, after declaring the importance of drawing up a European definition of robots, considers it appropriate to divide this concept into subcategories, see Annex to European Parliament resolution on Civil Law Rules on Robotics (note 10).

[40] Letter which the NHTSA, on 4 February 2016, sent to Chris Urmson, ex director of Google *self-driving car* Project (today Waymo), https://isearch.nhtsa.gov/files/Google%20–

so far to have already approved legislation on autonomous vehicles.[41] In Great Britain, a bill has been submitted but not yet approved.[42] Finally, there is now an *ad hoc* regulation at the European level, as already explained. However, there are several sector-specific regulations which could be applied analogously to issues relating to data protection in self-driving cars, until a specific EU legislation will be introduced.[43]

[Rz 28] What should be covered by the European legislation for the regulation of autonomous vehicles? What are the main aspects to be analysed and what are the desirable solutions? These questions require a wider discussion that we propose to deal with elsewhere. In this work, we focus on the consent to the processing of personal data in self-driving cars (*see* subparagraph 4.1 below), and rules on the design of such vehicles, in the light of privacy by design (*see* subparagraph 4.2 below).

4. Consent and Self-driving Cars

4.1. The (Ir)relevance of Consent to the Processing of Personal Data

[Rz 29] The consent of the data subject, as provided in recital 32 of the GDPR, is highlighted in a positive way. The GDPR rule is that the expresses consent is required for the processing of personal data (recital 32 GDPR), with the exception being explicit consent, which is required only with regard to special categories of personal data (art. 9 GDPR), profiling (art. 22 GDPR), and the transfers of personal data to a third country or an international organisation (art. 49 para. 1 lit. a GDPR). However, the difference between express and explicit consent is unclear and it would appear that explicit consent is nothing more than an express consent characterized by greater determination in the behaviour of the user.[44]

%20compiled%20response%20to%2012%20Nov%20%2015%20interp%20request%20–%204%20Feb%2016%20final.htm. Today, there are 33 States which have introduced *legislation related to autonomous vehicles*, as reported on http://www.ncsl.org/research/transportation/autonomous-vehicles-legislative-database.aspx.

[41] The German Federal Council approved the bill on autonomous driving, amending the Road Traffic Act. However, even with the introduction of new regulations, the driver is held liable in case of an accident. The framework of rules has been studied for an intermediate automation level (level 3 mainly). See Entwurf eines Gesetzes zur Änderung des Straßenverkehrsgesetzes, 20 February 2017, BT-Drucksache 18/11300.

[42] Vehicle Technology and Aviation Bill (Bill 143 2016-17), which would seem to appeal to the insurer's liability or the owner's liability in the event of a car accident involving.

[43] In addition to the GDPR are reported: on e-call systems Regulation (EU) 2015/758, Decision No 585/2014/EU and Regulation (EU) 305/2013; on Intelligent transport Systems (ITS) Directive 2010/40/EU and delegated Regulation; on electronic communications Directive 2002/22/CE, Directive 2002/21/CE, Directive 2002/20/CE, Directive 2002/19/CE and Directive 2002/58/CE (which could be replaced by Proposal for a Regulation of the European Parliament and of the Council COM(2017) 10 final of 10 January 2017 concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC). Furthermore, there are different initiatives which aim to regulate robotics and new technologies in general: besides European Parliament resolution on Civil Law Rules on Robotics (note 10), Declaration of Amsterdam (note 7), Proposal for a Regulation on Privacy and Electronic Communications (note 45), Communication from the Commission on the review of the digital single market strategy and White Paper on the Future for Europe, above mentioned, are cited COM(2016) 766 final on Cooperative Intelligent transport Systems (C-ITS), Letter of Intent of 23 March2017 on the testing and large scale demonstrations on Connected and Automated Driving (CAD), for the cooperation in the in the context of cross-border experiments on road safety, data access, data quality and reliability, connectivity and digital technologies, EU-U.S. Privacy Shield C(2016) 4176, which regulates the transfer of personal data for commercial purposes between Europe and the United States of America and the High Level Group for the automotive industry (GEAR) C(2015) 6943, which is very active in the field of automation.

[44] Caggiano (note 29), p. 11.

[Rz 30] In addition, recital 32 of the GDPR considers any positive act clearly indicating the willingness of the user to consent to the processing of his or her personal data as lawful, such as is the case of the consent provided online. This mode of consent is currently very common with the use of electronic means, where certain actions that appear to be more closely related to implied consent are accepted rather than the expressed consent (or even the explicit one). Taking the example of a website, sometimes it is not requested to tick a box indicating the user's consent when they are visiting a website, as long as in the banner that appears on the home page it is specified that the consent is deemed to have been provided simply by continuing to surf on the website. This does not match the definition of a positive act. Moreover, there are a few instances where consent is not required at all, as the Proposal for a Regulation on Privacy and Electronic Communications shows.[45] In the Proposal, the European Parliament and the Council critically analyse the Directive 2002/58/EC on electronic communications with particular regard to consent as the Directive has not reached its predetermined goals. In fact, end users face requests to accept so-called tracking cookies, without understanding their meaning and, sometimes, are even exposed to cookies being set without their consent.

[Rz 31] A study on this topic has been conducted to analyse the behaviour of the users required to give consent to the processing of their personal data to benefit from a service. It has been demonstrated that they generally provide consent without paying attention to the privacy notice.[46] In this way, the user's right to self-determination is undermined, since consent is not a freely given, specific, informed and unambiguous indication of the data subject's wishes.

[Rz 32] On the Internet of Things, a space where personal data is exchanged, and focusing on data exchanged between connected vehicles, the issue is further complicated. Indeed, while it is true that in some circumstances involving new technologies it is difficult to foresee expressed consent (and even more so explicit consent), we can easily imagine how much more complex it is to get this consent from users who are on board of an autonomous vehicle. It is therefore natural to ask oneself how and when the owner of the vehicle and any passengers on board should be informed about the processing of their personal data. In addition, it is important to wonder what form of consent is needed and whether this should be provided once or whenever the user or the passengers use the self-driving car.

[Rz 33] The right way could be the development of a specific framework of rules on self-driving cars. The framework should be applicable at least across the European Union and should protect users. A specific section should regulate the processing of user's personal data generated, stored and processed by connected vehicles. More specifically, it would be important to provide adequate and functional information to the users on the processing of their personal data (as required by the GDPR[47]), so that users know exactly what the consequences of the processing are. The privacy notice, to be adequate, cannot correspond to a standard model used for each type of processing. On the contrary, the privacy notice must contain information which is concise, transparent, intel-

[45] Proposal for a Regulation of the European Parliament and of the Council COM(2017) 10 final of 10 January 2017 concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC.

[46] The project is currently being carried out at Suor Orsola Benincasa University of Naples *Privacy and Internet of Things: a behavioural and legal approach.* For more detail about the project see Ilaria Amelia Caggiano, A Quest for Efficacy in Data Protection: A Legal and Behavioural Analysis, Working Paper no. 10/2017, p. 11 ff.

[47] The contents of the privacy notice are strictly listed in art. 13 and 14 GDPR. About the modality to act in accordance with the principle of transparency, see art. 12 and recital 58 GDPR.

ligible and easily accessible, written in clear and plain language, and free of charge. Indeed the privacy notice should be clear and understandable for an average user who, in this way, can be aware of the existence of the processing and its purposes, and of any profiling processes. Only in this way can the strong disinterest of users towards privacy notices be counteracted,[48] so that they can be effectively aware of the processing, protecting their interests to a lawful, fair and transparent processing. At the same time, the data controllers and processors will not be sanctioned for infringements of the GDPR.

[Rz 34] With regards to the consent to the processing of personal data, the framework of rules could overcome, in whole or in part, the requirement of consent, since this is no longer a lawful basis that guarantees the effectiveness of the data protection measures.[49] Among other things, in some cases, the law itself legitimises the processing of personal data without the need for consent, because of the fact that there are other more important interests at stake (other lawful base)[50], such as user's safety. Indeed, according to art. 6 para. 1 lit. d GDPR, the processing of personal data is lawful, even without the data subject's consent, when processing is necessary in order to protect the vital interests of the data subject or of another natural person, among which security may be included. An example is the eCall, an electronic device installed in the vehicle, which provides a free public service that can automatically make an emergency call to alert emergency services in the event of a traffic accident.[51] It is clear that the eCall, as a mandatory service, carries out a processing of personal data without the user's consent.[52] However, the data subject's protection is represented by the fact that the data is used for the sole purpose of dealing with emergency situations[53] and the call made only provides the minimum information for the rescue (such as the type of vehicle, the fuel used, the time of the accident, the exact localisation and the number of passengers on board).

[48] Introduction to Proposal for a Regulation on e-privacy and Electronic Communications; Caggiano (note 29), p. 1920; Jakub Misek, Consent to Personal Data Processing – The Panacea or the Dead End (2014), Masaryk University Journal of Law and Technology 8, p. 76 ff.

[49] Lucilla Gatt/Roberto Montanari/Ilaria Amelia Caggiano, Consenso al trattamento dei dati personali e analisi giuridico- comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali (2017), 2 Politica del diritto, p. 350–351; Caggiano (note 29), p. 20 ff.; Gabriela Zanfir, Forgetting About Consent: Why the Focus Should Be on «Suitable Safeguards» in Data Protection Law (2014), Reloading Data Protection, p. 237–257, https://ssrn.com/abstract=2261973. Art. 6 par. 1 lit. d GDPR states that, the processing of personal data is lawful – even without the consent – when processing is necessary in order to protect the vital interests of the data subject or of another natural person, among which security may be included.

[50] Misek (note 48), p. 79 ff.

[51] Regulation (EU) 2015/758 of the European parliament and of the Council of 29 April 2015 concerning type-approval requirements for the deployment of the eCall in vehicle system based on the 112 service and amending Directive 2007/46/EC [2015] OJ L123/77.

[52] According to art. 4 Regulation (EU) 2015/758, currently, the system is mandatory and therefore the consent to the processing of personal data is not requested. At the same time, explicit consent is needed to transfer personal data to any other third party. Anyways, it should be noted that data will not be disclosed to third parties without the consent of the data subject, and detailed technical regulation (including privacy by design) will prevent the exchange of personal data between the eCall system and third parties. Moreover, personal data is kept only for the time needed to deal with emergency situations and is completely deleted as soon as it is no longer needed; manufacturers ensure that the eCall system cannot be tracked or monitored and that data is automatically and permanently deleted from internal memory (art. 6 Regulation (EU) 2015/758). In contrast, see Art. 29 WP, Working document of 26 September 2006 on data protection and privacy implications in eCall initiative (2006), p. 5 ff., http://194.242.234.211/documents/10160/10704/ARTICOLO+29+-+WP+125-+eCall+initiative.pdf, where the Art. 29 WP took into consideration two options for the implementation of eCall (voluntary service or mandatory service). The first option evokesd consent to the processing of user personal data for a eCall service.

[53] Art. 5 para. 2 Regulation (EU) 2015/758, describes the type of road accidents involving the activation of the eCall system.

4.2. Data Protection by Design as a Special Tool for Strengthening ex ante Protection

[Rz 35] As it has already been argued in the preceding paragraphs, it is possible to collect personal data and develop a detailed profile of the subjects on board of the car (driver or passengers) and sometimes also third parties outside the car. Users are not always properly informed about the processing of their personal data or their possible profiling. What are the possible solutions?

[Rz 36] Even assuming consent of the data subject as a lawful basis for the processing of personal data has been achieved, a necessary addition to ensure the lawfulness of the processing is the strengthening of the user's effective monitoring over his or her personal data and the development of the principle of data protection by design, in addition to data protection by default (art. 25 GDPR).[54]

[Rz 37] The principle of data protection by design is a clear example of techno-regulation: at the time of the determination of the means for processing and at the time of the processing itself, the controller shall implement appropriate technical and organisational measures, which are designed to protect the users' privacy and security.[55] In the field of data protection by design, pseudonymisation has already been discussed as balancing the profiling process (*see* subparagraph 2.2 above) in order to allow transparent processing of personal data and only if necessary, but not to prevent it completely. It is therefore essential to have a more selective approach which is based on the notion of processing only information that is adequate, relevant and limited to what is necessary in relation to the purposes of the processing (i.e. data minimization, expressly provided by art. 5 para. 1 lit. c, and recalled in art. 25 GDPR about data protection by design). Thus, product performance and product safety are improved, and a useful market analysis is conducted.

[Rz 38] It should be remembered that pseudonymised data is not the same as anonymised data, given that the first one continues to allow the identification of the data subjects.[56] Nevertheless, within the data protection regulation (in which anonymisation in not regulated), pseudonymisation is an adequate *ex ante* protection tool, although having some exceptions.[57] Concretely, typical examples of pseudonymisation are the cryptography, the hash function (and its variants) as well as the tokenization.[58]

[54] The idea of using technologies to regulate technology itself and, in particular, aspects related to the protection of personal data, goes back to art. 17 Directive 95/46/EC, by introducing the technical and organizational measures that the controller should take to protect personal data. In those years, the Privacy Enhancing Technologies (PET) are being developed.

[55] Roberto D'Orazio, Protezione dei dati by default e by design (2016), La nuova disciplina europea della privacy (CEDAM 2016), p. 81 ff., points out that the principle of privacy by design cannot be applied absolutely and unconditionally but must «*take account of the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing*» (art. 25 para. 1 GDPR). At the same time, however, the data controller is required to adopt technical and organizational measures to ensure and demonstrate that the processing of personal data is implemented in compliance with the GDPR (art. 24 para. 1 GDPR), leading to a reversal of the burden of proof on the controller, in order to avoid the sanction under art. 83 and 84 GDPR.

[56] Art. 29 WP, Opinion 4/2014 of 10 April 2014 on surveillance of electronic communications for intelligence and national security purposes, p. 11.

[57] Yves-Alexandre De Montjoye/César A. Hidalgo/Michel Verleysen/Vincent D. Blondel, Unique in the Crowd: The Privacy Bounds of Human Mobility (2013), Scientific Reports 3:1376, https://www.nature.com/articles/srep01376.

[58] Art. 29 WP, Opinion 8/2014 (note 17), p. 21 ff.

[Rz 39] The increasing of data protection by design is one of the most important ways for guaranteeing the effectiveness of data protection. Moreover, the strengthening of privacy by design means that the requirement of consent could be overcome – at least specific and explicit consent, as opposed to generic consent when buying the self-driving car.

[Rz 40] In order to achieve this result, the lawyers should work in synergy with IT engineers in the development of autonomous driving systems and new technologies in general, complementing each other.

Maria Cristina Gaeta, Ph.D. candidate in People, Business and Market Law at University of Naples Federico II, member of the Research Centre of European Private Law (ReCEPL) and the Interdepartmental Centre of Project Design and Research Scienza Nuova, UTOPIA Lab. Via Porta di Massa, no. 32, 80133, Naples (Italy). mariacristina.gaeta@unina.it.