IOT, INTELLIGENT TRANSPORT SYSTEMS AND MAAS (MOBILITY AS A SERVICE)

Federico Costantini / Eleonora Archetti / Floridea Di Ciommo / Balint Ferencz

Researcher, University of Udine, Department of Law
Via Treppo 18, 33100, Udine, IT
federico.costantini@uniud.it; www.uniud.it

Temporary Agent, European Parliament

Co-director, cambiaMO research cooperative
c/Duque de Fernán Nuñez, 2, Madrid (ES)
floridea.diciommo@cambiamo.net

Ph.D. Student, Eötvös Loránd University, Faculty of Law
Egyetem tér 1–3, 1053 Budapest (HU)
balintov@caesar.elte.hu; www.ajk.elte.hu

Keywords: ***MaaS, Intelligent Transport Systems, Cyber Security, Data protection, Datex II***

Abstract: *IoT (Internet of Things) applications are crucial in Intelligent Transport Systems (ITS). MaaS (Mobility as a Service) is an advanced model of ITS in which public institutions, private operators and citizens are deeply connected since means of transport are virtualized in mobility resources and provided to users through the Internet. This contribution, after a short introduction, addresses legal concerns focusing on three aspects: (1) security of technological platforms and infrastructures, (2) protection of user's personal data, (3) communication among devices and in the IoT ecosystem.*

1. Introduction

Transport is a social phenomenon as old as humankind, which in recent years has been noteworthily changed due to the impact of «Information Society».

A transport system becomes «intelligent», according to European Union law, when information is not incidental or external, but a key element.[1] In an ITS (Intelligent Transport System) information is as important as the road, the wheel or the brake, since it shapes the «ecosystem» in which transport «systems» move goods and

[1] Intelligent Transport Systems (ITS) are defined «*systems in which information and communication technologies are applied in the field of road transport, including infrastructure, vehicles and users, and in traffic management and mobility management, as well as for interfaces with other modes of transport*», Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport, in OJ L 207, 6 August 2010, p. 1–13. In order to foster the application of such legal framework, the EU Commission has adopted five Delegated Regulations: 305/2013 of 26 November 2012 with regard to the harmonised provision for an interoperable EU-wide eCall, in OJ L 91, 3 April 2013, p. 1–4; 885/2013 of 15 May 2013 with regard to the provision of information services for safe and secure parking places for trucks and commercial vehicles, in OJ L 247, 18 September 2013, p. 1–5; 886/2013 of 15 May 2013 with regard to data and procedures for the provision, where possible, of road safety-related minimum universal traffic information free of charge to users, in OJ L 247, 18 September 2013, p. 6–10; 2015/962 of 18 December 2014 with regard to the provision of EU-wide real-time traffic information services in OJ L 157, 23 June 2015, p. 21–31; 2017/1926 of 31 May 2017 with regard to the provision of EU-wide multimodal travel information services, in OJ L 272, 21 October 2017, p. 1–13. See COM(2016) 766 final of 30 November 2016, An European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility. See also European Parliament resolution of 13 March 2018 on a European strategy on Cooperative Intelligent Transport Systems (2017/2067(INI)).

people.[2] In such an exchange of information among transport operators, services providers, public or private infrastructures and users, it is possible to observe a «proactive» pattern, since each agent adapts its strategies to the ecosystem.[3]

The cutting-edge version of ITS is called MaaS (Mobility-as-a-Service).[4] In it, the demand for transport is fulfilled providing a set of «virtualized» resources.[5] Given the global urbanization trend, such a model provides an alternative, flexible and sustainable metropolitan transportation system, allowing people to plan their multimodal journey and to travel without a personal car. In other terms, passengers can choose any means of transport to reach their destination, using either public service, private operators or shared vehicles. In MaaS, transport in itself becomes a kind of information, so we could argue that data become even more important than wheels.[6]

To sum up, the success of MaaS depends not only on a combination of heterogeneous components, but also on a strategic policy of balance between private sector and public interest and, most importantly, on the involvement of people. Users, in fact, have a key element of the system in their pocket. Without them, the system cannot work.

IoT (Internet of Things) can be considered an enabling technology in the development of «smart cities» and specifically in Intelligent Transport Systems.[7] Indeed, as confirmed by WP29 with special regard on personal data protection,[8] the control of devices, processes and systems raises several concerns: the control of information – and specifically about the security of the technological platform where it is managed – the protection of personal data of the community that uses such platforms – the accuracy of data of roads, traffic and travel – as a matter of travel safety – and the transparency and accountability of all processes involved.

In Maas such issues become more relevant due to the fact that, in it, «transport» becomes «mobility». In other words, if ITS can still be considered as a «mass» transport system, since it is provided indiscriminately to entire communities, MaaS aspires to offer «personal» mobility, targeting individual needs. To do so, it requires not only a larger amount of data, but also stronger control of information.

In a nutshell, the combination of IoT and MaaS generates a twofold intertwined network: on one side, interconnected «things»: data, devices, applications, infrastructures, vehicles of all sorts; on the other side, interconnected «people»: a community of travellers moving on the territory, each of them according to their

---

2 Experts classify three kind of ITS applications: Advanced Driver Assistance Systems (ADAS), Advanced Traveller Information Systems (ATIS) and Advanced Traffic Management Systems (ATMS), Ali/Ahmad/Malik/Ali/Rehman, Issues, Challenges, and Research Opportunities in Intelligent Transport System for Security and Privacy, Applied Sciences, volume 8, issue 10, 2018, p. 1–24.

3 In the next years ITS will evolve further and its deployment will spread worldwide. Its adoption is a specific strategy in the EU, see COM(2018) 283 final of 17 May 2018, On the road to automated mobility: An EU strategy for mobility of the future; see also Taiebat/Brown/Safford/Qu/Xu, A Review on Energy, Environmental, and Sustainability Implications of Connected and Automated Vehicles, Environmental Science & Technology, 2018.

4 Mobility-as-a-Service (MaaS) – or also Transportation-as-a-Service (TaaS) – has spread at a very fast pace since the introduction of its basic concepts by Sampo Hietanen and Sonja Heikkila, Hietanen, «Mobility as a Service» – the new transport model?, Eurotransport, volume 12, issue 2.- ITS & Transport Management Supplement, 2014, p. 2–4.

5 MaaS is characterized by four components: (1) infrastructure; (2) data providers; (3) transportation operators; (4) trusted mobility advisors. It is useful to analyze each of them separately, since they all play an important role in the structure of such a model of ITS; Goodall/Fishman/Bornstein/Bonthron, The rise of mobility as a service. Reshaping how urbanites get around, Deloitte Review, volume 20, 2017, p. 113–129.

6 https://en.wikipedia.org/wiki/Mobility_as_a_service (all websites last accessed on 4 January 2019). Some examples are «Whimp» used in Helsinki and UbiGo in Gothenburg; Karlsson/Sochor/Strömberg, Developing the «Service» in Mobility as a Service: Experiences from a Field Trial of an Innovative Travel Brokerage, Transportation Research Procedia, volume 14, 2016, p. 3265–3273; for a critical overview of MaaS experiences, see Kamargianni/Li/Matyas/Schäfer, A Critical Review of New Mobility Services for Urban Transport, Ibid., p. 3294–3303.

7 ITU, Recommendation ITU-T Y.2060 Overview of the Internet of things, 2012.

8 WP Opinion 8/2014 n. 223, adopted on 16 September 2014 on Recent Developments on the Internet of Things.

needs. «Internet of Things» and interconnected users are an open and complex network whose stability is exposed to any kind of perturbation.

In this paper we intend to focus on three main legal issues in MaaS, namely the security of ITS, the protection of personal data and the circulation of transport information.

2. ITS and cybersecurity

ITS is exposed to security flaws in very different ways. According to a recent study, fourteen different kind of vulnerabilities have been detected only for in-vehicle systems.[9]

In the public transport the problem is thorny, since the vastness of infrastructures required, the variety of technical architecture adopted by each operator, the lack of awareness by their personnel, the small budget devoted to protective measures. As emerges from an analysis of the European Network Information Security Agency (ENISA), five kinds of specific vulnerabilities can be identified.[10]

In MaaS, such issues are more complicated to implement since public and private operators are deeply intertwined in sharing data, platforms and application. Furthermore, a key element in this kind of services is the real-time geolocalization of vehicles and users. For this reason, a vulnerability affecting a single device, if hijacked, could spread and jeopardize an entire city in a very short time.

As an example of a security breach in ITS, it is useful to mention the ransomware attack suffered by the San Francisco Municipal Transportation Agency (MTA) in 2016,[11] in which more than 2 000 computers were infected. In that case, the consequences were marginal, as the metro management was forced to let passengers travel for free for some days, yet it was proved that the same weaknesses could be exploited with much more dangerous effects. In fact, shutting down escalators in rush hour could create queues so long to cause panic in the crowd, and changing traffic signals could deviate trains and cause a collision. Even minimal vulnerabilities can compromise an entire ecosystem and escalate in potential disasters.

The approach to cyber security adopted in recent years by the European Union is based on the concept of «resilience».[12] An institutional framework has been established in order to implement not only effective reactions to present threats, but also to prevent future risks and to promote a «proactive» strategy.[13]

Cyber security is a key concern also in ITS, as confirmed in Directive (EU) 2016/1148 of 6 July 2016,[14] which qualifies «operators of Intelligent Transport Systems» as «operator of essential services» (Annex II), including

---

9 Le/den Hartog/Zannone, Security and privacy for innovative automotive applications: A survey, Computer Communications, volume 132, 2018, p. 17–41, (p. 29). Such vulnerabilities can affect components (hardware or software), communication (internal or external) or environment.

10 Such vulnerabilities concern: scale and complexity of transportation networks, applying networked technology across large transport systems, multiple interdependent systems: access to real-time data, higher volumes of passengers and freight, Online passenger services; Lévy-Bencheton/Darra, Cyber Security and Resilience of Intelligent Public Transport, Good practices and recommendations, ENISA, Heraklion, 2016, (p. 27).

11 https://www.theguardian.com/technology/2016/nov/28/passengers-free-ride-san-francisco-muni-ransomeware.

12 It is noteworthy that «resilience» means the ability of a system to recover its ordinary balance after a perturbation, has become a key tenet in a wide range of EU policies, from disastrous natural events, to foreign diplomacy humanitarian crisis, to crime and terrorism.

13 See COM(2016) 410 final of 5 July 2016, Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry. See also Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises C/2017/6100, in OJ L 239, 19 September 2017, p. 36–58. The last recommendations provides a Blueprint for large-scale cyber crisis; see also the Proposal for a Regulation («Cybersecurity Act»), COM/2017/0477 final – 2017/0225 (COD), in which enforced rule is established for European Union Agency for Network and Information Security (ENISA).

14 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, in OJ L 194, 19 July 2016, p. 1–30, c.d. «Network Information Security» Directive.

them among the infrastructures to be safeguarded from incidents or attacks adopting a higher level of security measures.[15]

In a recent Communication[16] the European Commission has proposed to include the cyber security regulation as part of the revision of the General Safety Regulation for motor vehicles. In such perspective, in our view, security of information systems and safety in means of transport tend to combine in a joint control of all involved assets: databases, traffic infrastructures, in-vehicle technologies, hand-held devices, cloud applications, communication protocols. As the concept of «mobility» is a kind of renovated «transport», also new paradigms in security has to be developed.

3. ITS and data protection: the anonymity of MaaS passengers

Data protection has been taken into consideration by European institutions since the very beginning of ITS. Although the protection of personal data was included among the priority areas in the ITS Action Plan, it does not appear as such in «ITS Directive», where on the contrary we can find an indirect reference to «open data». Despite such an omission, pursuant the implementation of the ITS Action Plan, in 2014 the European Commission recommended the adoption of a «template for privacy impact assessments for ITS applications» and of a «Privacy-by-Design» philosophy.

In MaaS, the real possibility that the user could be not only profiled, but also «singled out», has raised many concerns. For example, it could be possible to find a pattern in a user's movements to and from healthcare facilities, and so correlate journey to certain illnesses. Furthermore, a user's destination could be a cult temple or the office of a syndicate, a political party or a civil organization. In such cases, and in many others, it seems that the guarantees provided by GDPR, either strictly legal (such as the consent of the data subject [Article 7 GDPR]), or technological (such as «Privacy by Design» [Article 25 GDPR]) are not suitable to avoid the risk that the «controller» or the «processor» could be punished accordingly.

Following the publication in 2017 of the *MaaS Alliance White Paper*,[17] which defines some basic principles on how data should be managed within the MaaS ecosystem, the Maas Alliance has recently published a more detailed document called *Data Makes MaaS Happen*.[18] In line with issues related to the development of C-ITS, the document states that the «*availability of data and interoperability of systems are prerequisites for actors in a MaaS ecosystem*».[19]

According to Art. 5 (1) of the GDPR, personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; and processed lawfully, fairly and in a transparent manner in relation to the data subject.

The same document is particularly relevant to understand the stakeholders' views on data flows and as a basis to analyse strengths and weaknesses in relation to the GDPR and the opinions given by the Article 29 Data Protection Working Party (WP) on specific issues like C-ITS and tracking. It identifies three use cases to demonstrate the data flows: a) the MaaS operator use case, b) the public transport use case and c) the traffic management use case. This distinction looks necessary not only for the sake of clarity, but especially in light of

---

15 For the implementation of the «N.I.S. Directive», by Member States, see COM(2017) 476 final/2 of 4 October 2017, Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union.

16 COM(2018) 283 final of 17 May 2018, On the road to automated mobility: An EU strategy for mobility of the future.

17 https://maas-alliance.eu/wp-content/uploads/sites/7/2017/09/MaaS-WhitePaper_final_040917-2.pdf.

18 https://maas-alliance.eu/wp-content/uploads/sites/7/2018/11/Data-MaaS-FINAL-after-plenary-1.pdf.

19 In its document, MaaS Alliance underlines the need of a high quality data being exchanged and lists ten purposes of processing data in order to provide a high standard service: 1) for user account management, 2) for optimal routing, 3) to provide the user with information on combined mobility solutions matching one's needs at that given moment, 4) for reservation and bookings, 5) to retrieve availability of vehicles, including car/bike/scooter-sharing fleet or rides, 6) for vehicle booking, 7) to unlock the vehicle, 8) for payment, 9) for digital ticketing, 10) to provide the user with solid time-critical information while planning and traveling.

the different purposes of processing personal data in MaaS. In fact, different purposes are likely to be grounded on different legal basis. With regard to the MaaS operator use case, the MaaS Alliance acknowledges that the most challenging process is the user account management. In order to comply with the principles enshrined in the GDPR and to respect the data subject rights, it is mandatory, for MaaS providers and operators, to deliver clear privacy statements. One of the ways to build up a solid trust between the service provider and the user would be, for example, to provide for a user-friendly access to personal data simultaneously to the delivery of the privacy statement.

With regard to the legal basis for data processing, three different possibilities seem to be more suitable to be applied: Art. 6 (1) (a) of GDPR (consent by the data subject), Art. 6 (1) (b) of GDPR (performance of a contract) or Art. 6 (1) (f) of GDPR (legitimate interest).

Of course, consent would seem the easier legal basis to apply. Yet it has to be considered not only that consent should be freely given, specific, informed, unambiguous, but also that the data subject has the right to withdraw it at any moment. In addition, the GDPR introduced other rules related to consent, which in some cases is required to be explicit (processing sensitive data, automated decision making, transfer of data to countries with non-adequate protection).

Also due to the drawbacks above observed, it seems that the data processing can be easily justified by the presence of a contract between MaaS provider and passengers.

More difficult to prove, but still possible, the processing could also be based on Art. 6 (1) (f) of GDPR. This legal basis is less used because the data process should pass the so called «legitimate interest assessment» that implies three steps:(1) Purpose test: what is the legitimate interest of the controller?(2) Necessity test: Is the processing necessary to achieve the purpose? (proportionality and subsidiarity test)(3) Balancing test: Do the individual's interests override the legitimate interest? If so, the legal basis of the legitimate interest cannot apply. In what way are the rights and freedoms of the individuals concerned at stake?

The GDPR requires to pay particular attention to the cases where the data subjects is a minor (therefore, the use of this legal basis looks risky in cases where the mobility service is addressed, for example, to families with children or schools). In general we can rely on this lawful basis to process personal data: if the use of personal data is proportionate, has a minimal privacy impact, and people would not be surprised (e.g. direct marketing), or where there is a compelling justification for the processing (e.g. security measures taken by a company).

As observed above, in MaaS, the real possibility that the user could be not only profiled, but also «singled out», has raised many concerns, in particular for the protection of special categories of data. Location data, so crucial for the success of MaaS, could easily become a metadata revealing special categories of data, the so called «sensitive data» listed at Art. 9 of GDPR.

It is therefore urgent that the new ePrivacy Regulation, still stuck at the Council, is adopted. In fact, the Art. 29 WP in its opinion of April 2017[20] welcomes the fact that the Proposed Regulation clearly covers content and associated metadata and recognizes that metadata may reveal very sensitive data. The WP keeps the same position in its subsequent Opinion on Processing personal data in the context of Cooperative Intelligent

[20] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610140; According to the WP, «*with regard to the analysis of content and metadata, the starting point should be that it is prohibited to process communications data without the consent of all end-users (senders and recipients). To allow providers to provide services explicitly requested by the user, such as for example search- and indexing functionality, or text-to-speech services, there should be a domestic exception for the processing of content and metadata for the purely personal purposes of the user him or herself. With regard to consent for tracking, the Working Party calls for an explicit prohibition on tracking walls, that is, take it or leave it choices that force users to consent to tracking if they want to have access to the service. Last but not least, the Working Party recommends that terminal equipment and software must by default offer privacy protective settings, and offer clear options to users to confirm or change these default settings during installation*».

Transport Systems (C-ITS).[21] The Art. 29 WP also confirms that data transmitted via C-ITS is personal data as the data subjects can be identified in various ways: 1) by the certificates they are provided by the Public Key Infrastructures, since those certificates will be unique by design; 2) by the location data themselves[22].

The Working Party identifies several technical possibilities to minimize the risks of reidentification:1) In order to prevent long term tracking, authorization tickets are changed over time.2) The frequency of broadcasting of Cooperative Awareness Messages needs to be adjusted. It is not enough that a vehicle changes its certificate, because it will still be possible to link the old and the new certificate.3) Respect of the data minimization principle, also by means of the application of remedies such as generalization or noise injection.

The WP identifies several risks related to the development of C-ITS. In fact «*kinematic and location data will be highly valuable to a number of interested parties with diverse intentions and purposes. Unrestricted and indiscriminate access to data shared within C-ITS may allow for the unfair accumulation of individual movement profiles, a ‹datification› of driving behaviours on which personalized goods and services can be shaped, advertised and sold. Mobility data may have the same appeal for law and traffic enforcement, beyond the purpose for which C-ITS data are generated and processed*».

Of course, we can acknowledge that, according to the GDPR, automated decision-making with legal effects or that significantly affect individuals may be acceptable if it is necessary for entering a contract or the performance of a contract between the data controller and data subject, or if the data subject gave explicit consent, as previously mentioned. It is also important to remember that automated decision-makings is acceptable if it is authorised by law and if the data subject's rights, freedoms and legitimate interests are fully safeguarded.

However, Art. 13 (2) (f) of the GDPR also provides that among the controller's obligations regarding the information to be provided where personal data are collected, data subjects must be informed about the existence of automated decision-making, including profiling.[23] The information should not only indicate the fact that there will be a profiling, but also contain meaningful information about the logic involved in the profiling and the possible consequences for individuals of the processing.[24]

4. ITS and data exchange: Datex II and blockchain

In this section we provide a description of the technologies involved in data transactions among devices in ITS, drawing a perspective on future possible implementations with blockchain technologies.

The aim of Directive 2010/40/EU is to pave the way for the Intelligent Transport Systems (ITS) technologies providing «*innovative services relating to different modes of transport and traffic management*» and enabling

---

21 Opinion 03/2017 of 4 October 2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS).

22 The WP underlines that «*the power of identification of location data is well known: just a few points in a path are enough to single out an individual in a population with a high degree of precision, taking into account the mostly regular patterns of people's mobility*». Article 29 Working Party highlights that the development of ITS technology, which will involve huge amounts of location data of individuals in Europe, creates new challenges to the fundamental rights and to the protection of personal data and privacy. As reminded by the WP, «*the C-ITS by concept will unveil where we drive and the way we drive. Intimate pieces of information will be publicly broadcasted to any nearby vehicle. This is a form of distributed permanent behavioural tracking which can generate an uncomfortable sense of stealthy surveillance*».

23 Article 29 Working Party (2017), Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP 251, 3 October 2017; Council of Europe, Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling, Art. 5 (5). The Recommendation includes provisions on the need to ensure that the processing in the context of profiling is fair, lawful, proportionate and carried out for specified and legitimate purposes. Consulting the CoE Recommendation could be particularly useful to figure out which information the controllers should provide to data subject.

24 For instance, a health insurance company using automated decision-making on applications should provide data subjects with general information on how the algorithm works, and which factors the algorithm uses to calculate their insurance premiums. Also when exercising their «right of access», data subjects can request information from the controller on the existence of automated decision-making and meaningful information about the logic involved.

«*various users to be better informed and make safer, more coordinated and ‹smarter› use of transport networks*» (paragraph (3) of the preamble). Among the delegated acts enacted by the EU Commission under Article 7 of the Directive, the above mentioned Regulation (EU) 2015/962 implements the DATEX II ontology in order to ensure the flawless communication between road-operators[25].

DATEX II is an ontology which fits into a chain of communicated traffic/road information written in XML/UML. The DATEX II has been developed for the road operators in order to provide a common understanding of data sent and received between each other. It is noteworthy that the DATEX II standard is deployed only between road-operators, while in order to ensure communication with the end-users another kind of communication model has been implemented. The content/service aggregators use the TPEG standard while the service providers and OEMs (Original Equipment Manufacturer) use the TPEG/C-ITS standard. These standards are set up to provide appropriate data schemes for the different actors of the mobility. However, these standards must be harmonized since if one part of the chain cannot treat some sort of data type which the other provide then the efficiency will be hard to maintain.[26]

The DATEX II model[27]covers the most relevant mobility aspects: roadworks, traffic management options, parking information, weather data, detector data per second or per vehicle, travel times, VMS settings, involved cars in accidents and characteristics of injured. These aspects are organized in three main parts: the «Common» namespace, the «LocationReferencing» namespace and the «Payloadpublication» namespace. The Common namespace contains the most basic elements of the data as Classes, DataTypes and Enumerations. The LocationsReference in line with its name provide data scheme for the various elements of location. The PayLoadPublication possess the «Parking», the «RoadTrafficData», the «Situation» and the «VMS» part so the real important data schemes for the outside world take places here.

As we have noted above, one of the key issue is the interchangeability of the data based on the different data schemes (DATEX II, TPEG, TPEG/C-ITS). For example back in 2013 there was problem between TPEG-DATEX II namely that the TPEG may distinguish warning levels regarding problems in the road whereas in «*the current version of DATEX II has no possibility to mark message as «safety relevant»*[28].

Concerning the future perspectives, it is common opinion that blockchain and smart contracts technologies will bring many advantages: reducing tremendously costs of transactions, integrating payment systems and KYC (know-your-customer) procedures. Furthermore, they can improve trust among commercial partners in several kind of transactions – Business to Business (B2B), Business to Customer (B2C) and Customer to Customer (C2C) – without intermediators. In a report IBM has observed that – particularly in the field of

---

[25] According to Article 5 of the delegated Regulation «*For the purpose of facilitating the provision of compatible, interoperable, and continuous real-time traffic information services across the Union, road authorities and road operators shall provide the dynamic road status data they collect and update pursuant to Article 9 in DATEX II (CEN/TS 16157 and subsequently upgraded versions) format or any machine-readable format fully compatible and interoperable with DATEX II*» and this provision is reiterated in the Article 6 for the traffic data. In Article 9 and Article 10 the delegated regulation identifies what sort of data must be updated and how it must be done.

[26] The DATEX II model is built upon three layers named level A, level B and level C. The level A is the core of the data model which may be modified only by upgraded version of the DATEX II model. The level B aims to provide possibility to amend or enhance the level A layer. While the level C makes the model more flexible with the opportunity to make a quite completely independent layer from them level A but allows to still make the part of the DATEX II model.

[27] See the current DATEX II version here: http://d2docs.ndwcloud.nu/_static/umlmodel/v3.0/index.htm.

[28] Safety related message sets – Selection of DATEX II Codes, TPEG2-TEC-Causes and TCM events for EC high level categories (http://tisa.org/wp-content/uploads/ITSTF13004_SafetyrelatedMessage-Sets-DATEXII-TPEG-TECandTMC_v3.pdf). In 2018 in Utrecht the DATEX II forum was held and as an outcome a 10 point declaration has been adopted. Among them the following statements deserve to be mentioned: (1) DATEX II is an important backbone to enable C-ITS. Close cooperation is needed between C-ITS – DATEX II – OEMs in order to develop interoperable harmonized profiles. (2) DATEX II Light will improve innovation and accelerate deployment of end-user services driven by the open data community. (3) The DATEX II data dictionary should be published in a natural language. In this light, further innovation may be expected for DATEX II especially regarding the interoperability between other data schemes, https://www.datex2.eu/node/789.

car-sharing – the deployment of smart contracts may widen the possibilities how and what may be offered to customers.[29]

With specific regard to MaaS, blockchain technology may initiate a breakthrough due to its efficiency and relatively fast widespreading. Blockchain may render it possible to deploy smart contracts on the blockchain which make payment and exchange other services in a somewhat fast and convenient way. Since the blockchain technology may storage, share and check data in a different manner than centralized technology does, it enables to maintain privacy of the customers while through the new way of sharing data it can handle the hardships which may derive from the variety of the customer's habits and customs regarding the mobility and the services provided for them. Blockchain makes the opportunity to connect the fragmented nature of the services currently on the field although it is hard to predict how the legal systems may treat smart contracts and payments upon that.[30] There is doubt whether the blockchain technology and GDPR provisions are in line with each other.[31]

There are already several start-ups and platforms in this sector:[32] Car eWallet (to handle tolls, parking, electric vehicle charging, car sharing and in-car services), Tesseract (mobility platform with transport services ranging from single vehicles to fleets available on the platform), DAV, Share&Charge, Streamr, and there are many other initiation in usage-based insurance and automative security & privacy.

On the other hand it is quite hard to say if the key figures are really committed to use this sort of technology. In this year the IBM Institute for Business Value, in collaboration with Oxford Economics issued a survey in which 1 314 automotive executives across 10 functional areas and 10 countries have been asked about the possible implementation of blockchain technology.[33] According to this survey «*only a small number of OEMs and suppliers are currently ready for blockchain or have blockchain solutions that are ready for commercial use*».[34] One question explicitly regarded the MaaS field asking if the executives expect blockchain to impact business models in number of areas (including Maas).[35] From behalf of the OEMs the highest number of executives expect it from China, India, Japan, Germany, Mexico and the USA (50%–75%). However, from the suppliers' side only the German and American executives seem to agree to such vision.

5. Conclusions

The technologies upon which ITS is built include autonomous vehicles, next-generation ICT connectivity, telecommuting / telehealth, user apps, Big Data, intelligent processing, advanced manufacturing (including 3D printing), Internet of Things, novel materials and embedded sensors in infrastructure.[36]

MaaS is a special application of ITS and most of the time it is a user app that represents a kind of peer-to-peer system, potentially possible thanks to the technological platforms. However, the initial «horizontal» aspect (i.e. peer-to-peer) is lost when the owner of a technological platform is one single agent who is using relevant information for creating added-value to sell to transport MaaS end-users and MaaS provider. Processing data of the MaaS end-user (peer) in order to provide him a high standard service from a MaaS provider (peer) means

[29] Blockchain for mobility services – Personalized mobility through secure data (https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBE03891USEN).

[30] See recently: Werbach/Cornell, Contracts Ex Machina, Duke Law Journal, volume 67, 2017, p. 313–382, Kolber, Not-So-Smart Blockchain Contracts and Artificial Responsibility, Stanford Technology Law Review, volume 198, issue 21/2, 2018, p. 198–234.

[31] https://www.coindesk.com/7-legal-questions-that-will-define-blockchain-in-2019 (Jenny Leung, 3 January 2019).

[32] https://medium.com/datadriveninvestor/how-can-blockchain-technology-disrupt-the-auto-industry-8bfe091467c3 (Suhasini Gadam, 22 April 2018). The examples have been taken from the article.

[33] Daring To Be First – How auto pioneers are taking the plunge into blockchain (https://www-935.ibm.com/services/us/gbs/thoughtleadership/autoblockchain/index.html)

[34] Ibid, p.3.

[35] Ibid, pp. 9–10.

[36] Rohr/Ecola/Zmud/Dunkerley/Black/Baker, Travel in Britain in 2035, Rand Corporation, Santa Monica-Cambridge, 2016, (p. 8); Rohr/Ecola/Zmud/Dunkerley/Black/Baker, Travel in Britain in 2035, Rand Corporation, Santa Monica-Cambridge, 2016, (p. 8).

creating additional vulnerabilities. For example, the improper use of sensitive data related to pattern trips (i.e. various origin-destinations such healthcare facilities, cult temple or the office of a syndicate, a political party or a civil organization, children school) is a legal concern.

In such cases, and in many others, it seems that the guarantees provided by GDPR, either strictly legal, or technological are not welcome by the «controller» or the «processor» of MaaS platform. The bottom line is that the more technology you add, the more data you produce, the more vulnerabilities you end up creating. For example, minimal vulnerability can compromise the security of technological platforms and infrastructures with the entire ecosystem (see the Metro issue in San Francisco in 2016). The only way to minimize this vulnerability is to prevent future risks and promote a proactive strategy for making the Information Transport System more resilient. The legal framework needs to support as well the communication among devices in an IoT ecosystem, therefore a DATEX II ontology has been implemented for facilitating the provision of compatible, interoperable, and continuous real-time traffic information services across the Union where road authorities and road operators shall provide the dynamic road status data they collect and update.

The general conclusion of this article suggests that ITS generation of data should be treated such as our DNA data whose circulation could not be left to the single agent or owner of platforms that per se create vulnerabilities at the basis of a progressive loss of socio-economic protections and democracy guaranties.

6. Acknowledgement

This paper is the outcome of a Short Term Scientific Mission held in Madrid within the COST ACTION 16222 Wider Impacts and Scenario Evaluation of Autonomous and Connected Transport https://www.cost.eu/actions/CA16222/, http://wise-act.eu

7. References

Ali, Qazi/Ahmad, Naveed/Malik, Abdul/Ali, Gauhar/Rehman, Waheed, Issues, Challenges, and Research Opportunities in Intelligent Transport System for Security and Privacy, Applied Sciences, volume 8, issue 10, 2018, p. 1–24.

Goodall, Warwick/Fishman, Tiffany Dovey/Bornstein, Justine/Bonthron, Brett, The rise of mobility as a service, Reshaping how urbanites get around, Deloitte Review, volume 20, 2017, p. 113–129.

Hietanen, Sampo, «Mobility as a Service» – the new transport model?, Eurotransport, volume 12, issue 2.-ITS & Transport Management Supplement, 2014, p. 2–4.

ITU, Recommendation ITU-T Y.2060, Overview of the Internet of things, 2012.

Kamargianni, Maria/Li, Weibo/Matyas, Melinda/Schäfer, Andreas, A Critical Review of New Mobility Services for Urban Transport, Transportation Research Procedia, volume 14, 2016, p. 3294–3303.

Karlsson, I. C. MariAnne/Sochor, Jana/Strömberg, Helena, Developing the «Service» in Mobility as a Service: Experiences from a Field Trial of an Innovative Travel Brokerage, Transportation Research Procedia, volume 14, 2016, p. 3265–3273.

Kolber, Adam J., Not-So-Smart Blockchain Contracts and Artificial Responsibility, Stanford Technology Law Review, volume 198, issue 21/2, 2018, p. 198–234.

Le, Van Huynh/den Hartog, Jerry/Zannone, Nicola, Security and privacy for innovative automotive applications: A survey, Computer Communications, volume 132, 2018, p. 17–41.

Lévy-Bencheton, Cédric/ Darra, Eleni, Cyber Security and Resilience of Intelligent Public Transport. Good practices and recommendations, ENISA, Heraklion, 2016.

Rohr, Charlene/Ecola, Liisa/Zmud, Johanna/Dunkerley, Fay/Black, James/Baker, Eleanor, Travel in Britain in 2035, Rand Corporation, Santa Monica-Cambridge, 2016.

Taiebat, Morteza/Brown, Austin L./Safford, Hannah R./Qu, Shen/Xu, Ming, A Review on Energy, Environmental, and Sustainability Implications of Connected and Automated Vehicles, Environmental Science & Technology, 2018.

Werbach, Kevin/ Cornell, Nicolas, Contracts Ex Machina, Duke Law Journal, volume 67, 2017, p. 313–382.