Title: "Balancing Data Sharing, Privacy, and Cybersecurity in Smart Mobility"

Introduction and Context:

The recent evolutions in the mobility sector bring many potential beneficial use cases of data sharing. Cloud computing infrastructures and AI systems can be used to analyse shared data and contribute to improved traffic management, enhanced vehicle safety, and other overall societal benefits (smart charging for electric vehicles, etc.). While data produced by connected cars were initially intended to enhance vehicle functions, they can also be used for many other purposes, including added commercial services (autonomous driving, on-board functions) but also government services (planning of road inspections, maintenance of mobility infrastructures or informing public policy related to mobility) (Schellekens, 2022; Coppola and Morisio, 2017).

However, these use cases raise various challenges, including the need to promote data sharing in the mobility sector while ensuring the coherence of a very rich and complex legal ecosystem (**I**) and the need to find legal and technical solutions to guarantee cyber-secured and privacy-preserving data sharing practices in smart mobility use cases (**II**).

I – Data sharing promotion through adapted and consistent regulations

First, to allow innovation in "smart mobility" to develop its full potential, data sharing is key and needs to be facilitated through adapted legal frameworks and relevant technical solutions. Indeed, when it comes to connected vehicles, the car manufacturer finds itself in a "gatekeeper" position, holding all the generated data and being the only one having the technical capacity to process, share or monetize the data. From a competition perspective, this situation is not satisfying as new entrants or non-manufacturers do not have the ability to innovate in the mobility sector without access to these data (Kerber, 2019). That is why data sharing needs to be encouraged through adapted policy initiatives (D'Agostino *et al.*, 2019; Kerber, 2018).

The currently discussed or recently adopted European regulations promoting personal and non-personal data flows seem to contribute to that goal but their practical implications remain uncertain. For instance, the Data Governance Act[1] will likely create new actors on the data market defined as "data intermediaries" which are supposed to act as "trusted" data brokers. Meanwhile, the Data Act[2], which has been adopted on December 13th, 2023, and which will be fully applicable on September 12th, 2025, will force connected products (including those used in connected vehicles) manufacturers to make data available to users "by default". The latter will also be granted the right to ask data holders to share their data with third parties, specifically data processing services providers. **What will be the consequences of these new regulations, whose objective is to encourage data sharing and the free flow of data within the EU, in the mobility sector?** In addition, this sector is subject to a great number of vertical, sector-specific, regulations like the Intelligent Transport Systems Directive[3]. The proposed thesis will

[1] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act).
[2] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act).
[3] 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 (ITS Directive).

need to **identify and study all sectorial regulations which may have an impact on data sharing practices (see for example Kerber and Gill, 2019), in order to determine how they would interoperate with the new horizontal European regulations**.

II – Securing privacy and cybersecurity risks while promoting data sharing in the mobility sector

Apart from the regulatory consistency issues mentioned above, data sharing in the mobility sector brings risks for individual rights, privacy and cybersecurity. Indeed, some personal data produced by connected vehicles are intrusive by nature, such as the real-time personal location or the car model purchased. Others may be indirectly intrusive as they may reveal, through data analysis techniques, sensitive information such as life habits, driving style, periods of absence from home, personal and professional addresses. These highly personal information can be inferred, for example, from the analysis of electric vehicles' load curves or from the track-record of charging stations used by the driver. This is the reason why data security is so important when it comes to mobility use cases. Cyber risks have been extensively documented in scientific literature (Salek et al., 2022), and need to be constantly updated due to accelerated technological development and new threats such as AI or quantum computing.

The proposed thesis should aim at **identifying all these risks, studying the solutions to minimise them (through Privacy-enhancing-technologies) and proposing solutions (including legal reforms and/or technical solutions) to strike a balance between data accessibility, privacy and cybersecurity**.

From the legal point of view, European laws indeed already set safeguards to protect data generated by connected vehicles. The most obvious is the General Data Protection Regulation[4] (GDPR) which regulates personal data collection and processing, including in the mobility sector (Manny, 2018). However, its application to connected cars raises various challenges concerning, for example, the identification of the "data controller" among multiple stakeholders (Zallone, 2019), the legal basis that can be used to collect data, including consent and legitimate interest, or the individual right to object the processing (Pizzi, 2017). The GDPR also contains a security obligation[5] which requires data controllers to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, such as pseudonymisation or data encryption. To help stakeholders translating these obligations in the mobility sector, data protection authorities issued recommendations (CNIL, 2017; EDPB, 2021), which confirm the sensitive nature of mobility data. In parallel, cybersecurity regulations continue to expand, such as NIS 2 directive[6], and bring with them additional regulatory restrictions to data sharing.

For now, this complex legal ecosystem is hard to navigate. Recently, the Court of Justice of the European Union ruled against a car manufacturer, Fiat Chrysler, which required a payment and other conditions from independent garages to access maintenance data[7]. The EUCJ did not

[4] Regulation (EU) 2016/679 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 (General Data Protection Regulation).
[5] GDPR, article 32.
[6] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the union, amending regulation (eu) no 910/2014 and directive (eu) 2018/1972, and repealing directive (EU) 2016/1148 (NIS 2 Directive).
[7] EUCJ, Case C-296/22, A.T.U. Auto-Teile-Unger GmbH & Co. KG, Carglass GmbH v. FCA Italy SpA, October 5th, 2023.

accept the security concerns raised by Fiat Chrysler and clarified that security measures must not restrict access to the data. This shows a strong dynamic, including in the mobility sector, in favour of data accessibility. This suggests that car manufacturers will have to prepare themselves for a new era where vehicle data must be much more accessible.

Usual solutions outside the sharing scenario consist in protecting servers and data from cyberattacks, thanks to cybersecurity tools such as Intrusion Detection Systems, firewalls, data encryption, etc. But when it comes to sharing sensitive and personal data while complying with the legal frameworks, it is compulsory to implement the principle of "privacy by design", mainly based on privacy enhancing technologies (PETs). In this way, the data is encoded in such a way that only authorized processing is possible, and only by authorized entities. This prevents the data controller from abusing its prerogatives, or a malicious actor from accessing the shared data. There are currently several possibilities of PETs that could be relevant in the context of smart mobility.

One solution could be to use advanced protection tools, allowing to work to be performed on encrypted information, such as homomorphic encryption (Gentry, 2009), secure multiparty computation (Yao, 1982), functional encryption (Goldwasser et al., 2013). Another possibility consists in interacting with a hardware secure element (CCC, 2024) that is responsible for the manipulation of any sensitive data, at any time. We could also apply a configurable form of anonymity/pseudonymity such as Differential Privacy (Dwork et al., 2006) or K-Anonymity (Samarati et al., 1998).

The objective of this research thesis is to combine these methods to propose innovative solutions that are more adapted than the existing systems to the case of data sharing in smart mobility systems. It will compare the advantages and drawbacks of the proposed methods in terms of security/privacy contributions, data usability, and their counterparts in terms of efficiency and practicality. These solutions will consider portability and will follow a stronger security model (following the "privacy by design" principle), in coherence with the legal aspects.

Conclusion

While the free flow of data is displayed as a clear objective of European policy, other regulations seem to discourage data sharing for privacy or cybersecurity considerations. Regulatory restrictions to data sharing need to be studied to determine their concrete impact on smart mobility use cases and on their multiple stakeholders (vehicle manufacturers, software developers, users…).

That being done, we should find the most appropriate security and privacy tools to protect sensitive and personal data, in a privacy by design way, to comply with legal restrictions.

Hence, the thesis should aim at **proposing concrete solutions for all stakeholders to reconcile the competing objectives of data sharing promotion and privacy and cybersecurity risks prevention**. Taking this into consideration, the main goal of the research is to propose an analysis that not only navigates the complexities of the legal framework but also aligns with the spirit of emerging European regulations, propose technical solutions for data protection, and contribute to ensuring a secure future for beneficial use case in the mobility sector for the public good.

Proposed methodology

1. **Case study analysis (Year 1 + 2)**: During the first year, the candidate is expected to identify and analyse case studies of existing data sharing practices in the smart mobility sector. This analysis will involve examining different models of data sharing, their implications for privacy and cybersecurity, and the regulatory frameworks governing them. This could be done in collaboration with partners of the IMCS chair and by engaging in interviews with relevant stakeholders including government agencies, industry associations, legal experts, and civil society organizations. These consultations will provide valuable insights into the practical challenges and concerns surrounding data sharing, privacy, and cybersecurity in smart mobility.

2. **Literature review (Year 1 + 2)**: The candidate is also expected, during the first and second years, to conduct an extensive literature review on relevant legal frameworks, regulations, and academic papers related to data sharing and PETs (privacy, and cybersecurity) in smart mobility. This will involve mapping and studying sectorial regulations in the transportation sector (ITS directive, etc), and horizontal regulations related to data protection (GDPR, Data Act, Data Governance Act) or cybersecurity (NIS 2, etc). The candidate will need to analyse the impact of these regulations on cybersecurity and data sharing practices in smart mobility use cases (I), and to understand, for each privacy and security tool, how it could be a solution to comply with those regulations by appropriately protecting sensitive and personal data (II).

3. **Proposals development (Year 2)**: Based on the findings from the literature review, case studies and stakeholder consultations, the candidate will develop proposals for legal reforms and/or technical solutions aimed at balancing data accessibility, privacy, and cybersecurity in smart mobility. This may involve drafting model regulations, policy recommendations, guidelines for industry best practices, or new ways to use technical solutions.

4. **Thesis writing (Year 3)**: The third year will be dedicated to writing the PhD thesis. The thesis will present a comprehensive analysis of the regulatory landscape, identify inconsistencies, gaps and challenges, and propose innovative solutions for achieving a balance between data sharing, privacy, and cybersecurity in smart mobility.

This methodology provides a structured approach for conducting interdisciplinary research in law, combining legal analysis with other social sciences methods such as empirical research to address questions at the intersection of technology, regulation, and society.

Bibliography:

Acharya S., Mekker M. (2022). Measuring data sharing intention and its association with the acceptance of connected vehicles, *Transportation Research Part F: Traffic Psychology and Behaviour*, Volume 89, 423-436, https://doi.org/10.1016/j.trf.2022.07.014.

Confidential Computing Consortium (2024). https://confidentialcomputing.io/about/.

CNIL. (2023). Club conformité véhicule connecté et mobilité – Compte-rendu de l'atelier n°1 « Compréhension des enjeux économiques et concurrentiels des traitements de données concernés », April 2023, online: https://www.cnil.fr/sites/cnil/files/2023-07/club_conformite_vehicules_connectes_et_mobilites_compte_rendu_atelier_du_21_avril_2023.pdf.

CNIL. (2017). Connected Cars and Personal Data, Compliance Package, October 2017, online: https://www.cnil.fr/sites/cnil/files/atoms/files/cnil_pack_vehicules_connectes_gb.pdf.

Coppola R., Morisio M. (2017). Connected Car: Technologies, Issues, Future Trends. *ACM Computer Survey*, Volume 49, Issue 3, Article n°46, https://doi.org/10.1145/2971482.

D'Agostino M., Pellaton P., Brown A. (2019). Mobility Data Sharing: Challenges and Policy Recommendations. *UC Davis: Institute of Transportation Studies*, Issue Paper, August 2019. https://escholarship.org/uc/item/4gw8g9ms

Dwork C., McSherry F., Nissim K., Smith A. (2006). Calibrating Noise to Sensitivity in Private Data Analysis, Theory of Cryptography Conference, 2006. https://link.springer.com/chapter/10.1007/11681878_14.

EDPB. (2021). Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, March 2021, online: https://edpb.europa.eu/system/files/2021-03/edpb_guidelines_202001_connected_vehicles_v2.0_adopted_en.pdf

Gentry C. (2009). Fully Homomorphic Encryption Using Ideal Lattices, Symposium on Theory of Computing, 2009, https://dl.acm.org/doi/10.1145/1536414.1536440.

Gill D., Metzger J. (2022). Data access through data portability: economic and legal analysis of the applicability of art. 20 GDPR to the data access problem in the ecosystem of connected cars. *European Data Protection Law Review (EDPL)*, 8(2), 221-237, https://doi.org/10.21552/edpl/2022/2/9.

Gill D. (2022). The Data Act Proposal and the Problem of Access to In-Vehicle Data and Resources. *Available at SSRN*: https://ssrn.com/abstract=4115443.

Goldwasser S., Kalai Y., Ada Popa R., Vaikuntanathan V., Zeldovich N. (2013). Reusable garbled circuits and succinct functional encryption, Symposium on Theory of Computing, 2013. https://dl.acm.org/doi/10.1145/2488608.2488678.

Kerber W., Gill D. (2019). Access to Data in Connected Cars and the Recent Reform of the Motor Vehicle Type Approval Regulation. *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 10(2), 244, https://dx.doi.org/10.2139/ssrn.3406021.

Kerber W. (2018). Data governance in connected cars: the problem of access to in-vehicle data. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 9(3), 310-331, https://ssrn.com/abstract=3285240.

Kerber W. (2019). Data sharing in IoT ecosystems and competition law: the example of connected cars. *Journal of Competition Law and Economics*, 15(4), 381-426, https://dx.doi.org/10.2139/ssrn.3445422.

Krompier J. (2017). Safety first: the case for mandatory data sharing as federal safety standard for self-driving cars. *University of Illinois Journal of Law, Technology & Policy*, 2017(2), 439-468.

Salek M. S. *et al*. (2022). A Review on Cybersecurity of Cloud Computing for Supporting Connected Vehicle Applications. *IEEE Internet of Things Journal*, 9(11), 8250-8268, doi: 10.1109/JIOT.2022.3152477.

Samarati P., Sweeney L. (1998). Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression, Technical Report SRI-CSL-98-04, 1998. http://www.csl.sri.com/papers/sritr-98-04/

Manny C. (2018). Driven Data: Connected Cars and Privacy Law. *Business Law Review*, 51, 35-56.

Peacher H.B. (2020). Regulating Data Privacy of Connected Vehicles: How Automotive Giants Can Protect Themselves and Their Golden Goose. *Albany Law Journal of Science & Technology*, 30, 74.

Pizzi P. J. (2017). Connected cars and automated driving: privacy challenges on wheels. *Defense Counsel Journal*, 84(3).

Schellekens M.. (2022). Data from connected cars for the public cause, *Computer Law & Security Review*, Volume 45, 105671, https://doi.org/10.1016/j.clsr.2022.105671.

Unekbas S. (2023). Verticalization of data sharing and the difficult path to 'EUnnovation'. *Market and Competition Law Review*, 7(2), 131-166.

Wiegand N., Schmalenberger A. (2023). Access to vehicle data: A look at the recent decision of the European Court of Justice. *Taylor Wessing (blog)*, online: https://www.taylorwessing.com/en/insights-and-events/insights/2023/10/access-to-vehicle-data.

Xiong J., Bi R., Zhao M., et al. (2020). Edge-Assisted Privacy-Preserving Raw Data Sharing Framework for Connected Autonomous Vehicles. *IEEE Wireless Communications*, 27(3), 24-30, doi: 10.1109/MWC.001.1900463.

Yao A.C. (1982). Protocols for secure computations, Symposium on Foundations of Computer Science, 1982. https://ieeexplore.ieee.org/document/4568388.

Zallone R. (2019). Connected Cars under the GDPR. *2019 AEIT International Conference of Electrical and Electronic Technologies for Automotive (AEIT AUTOMOTIVE)*, Turin, Italy, doi: 10.23919/EETA.2019.8804515.