Designing Connected and Automated Vehicles around Legal and Ethical Concerns: Data Protection as a Corporate Social Responsibility

Paolo Balboni*
paolo.balboni@maastrichtuniversity.nl
Maastricht University – Faculty of Law – Private Law
Bouillonstraat 3, 6211 LH Maastricht, The Netherlands
paolo.balboni@ictlegalconsulting.com
ICT Legal Consulting
Via Borgonuovo 12, 20122 Milan, Italy

Anastasia Botsi
anastasia.botsi@ictlegalconsulting.com
ICT Legal Consulting International
Piet Heinkade 55, 1019 GM Amsterdam, The Netherlands

Kate Francis
kate.francis@ictlegalconsulting.com
ICT Legal Consulting
Via Borgonuovo 12, 20122 Milan, Italy

Martim Taborda Barata
martim.tabordabarata@ictlegalconsulting.com
ICT Legal Consulting International
Piet Heinkade 55, 1019 GM Amsterdam, The Netherlands

ABSTRACT

Emerging technologies and tools based on Artificial Intelligence (AI), such as Connected and automated vehicles (CAVs), present novel regulatory and legal compliance challenges while at the same time raising important questions with respect to ethics and transparency.

On the one hand, CAVs bring to light theoretical and practical challenges to the implementation of the multi-dimensional obligations of the current European personal data protection legal framework, including the General Data Protection Regulation (GDPR), the ePrivacy Directive,[1] and where applicable, the Directive for a high common level of security and information systems (NIS Directive or NISD).[2] As mere examples, CAV developers currently face multiple legal hurdles to overcome, including the necessity to fulfil controller and/or processor obligations in complex data processing scenarios[3] and tensions with the GDPR's principle of purpose limitation[4] (which comes at odds with the autonomous processing of personal data through AI in the CAV, which may be based on a (re)interpretation of goals, or, possibly, a shift in focus from the original goal for which personal data was collected). Additionally, the overall need for relatively large datasets to properly train and leverage AI functionalities leads to conflicts with the principle of data minimization.[5] When applied to AI systems, the requirement of data protection by design and by default also presents difficulties, as data protection by default is possible only when the necessary personal data is processed for a specific purpose.[6] Moreover, the ePrivacy Directive has been interpreted by European Supervisory Authorities – notably, the European Data Protection Board (EDPB)[7] – as requiring a company wishing to store or access information stored within a CAV to obtain specific consent from CAV users for these specific activities. Furthermore, an additional legal basis must be determined (possibly necessitating those companies to make a double request for consent) for any subsequent use of the information stored or accessed, such as the analysis of telematics data collected from a CAV. This interpretation creates challenges at the technical and legal levels in particular where the legal basis defined for subsequent use of CAV information is *not* consent, such as in the case of pay-as-you-drive insurance, where the contract entered into between the CAV user and an insurance company serves as a legal basis for the processing of their personal data. A conflict between the legal basis used for information storage/access – consent, which

[*] Prof. Dr. Paolo Balboni is Professor of Privacy, Cybersecurity, and IT Contract Law at the European Centre on Privacy and Cybersecurity (ECPC) within the Maastricht University Faculty of Law and Founding Partner of ICT Legal Consulting.

[1] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

[2] The NISD, applicable to *operators of essential services* and *digital service providers,* ensures the security of network and information systems vital to economic and societal activities and to the functioning of the internal EU market. Also see Recital (1) NISD.

[3] Under the GDPR there are two main roles that an organization can take on regarding an activity which involves the processing of personal data: that of controller, or that of processor. Article 4 (7) GDPR defines controller as "*the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data*"; where two or more controllers jointly determine the purposes and means of a given processing activity, they will be considered as "*joint controllers*" under Article 26 GDPR. Article 4(8) GDPR defines processor as "*a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*". Depending on the data protection role which is applicable to an organization, its obligations will change, as can be better seen in Articles 25 to 28 GDPR.

[4] According to Article 5(1)(b) GDPR, the personal data must be "*collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes*".

[5] The principle of data minimization according to Article 5(1)(c) GDPR, requires that personal data are processed to the extent to which it is "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*".

[6] Commission Nationale Informatique & Libertes, *Compliance Package: Connected vehicles and personal data.* October 2017. Available at: https://www.cnil.fr/sites/default/files/atoms/files/cnil_pack_vehicules_connectes_gb.pdf.

[7] European Data Protection Board, *Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications.* 28 January 2020. Available at: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf.

WAIEL2020, September 3, 2020, Athens, Greece

must be freely withdrawable under the GDPR[8] – and the legal basis used for information use – e.g., performance of a contract, which will typically not be compatible with the possibility for the CAV user to freely prevent the insurance company from continuing to process their personal data emerges in this context. Concerns from the data security[9] perspective are also highly relevant, notably due to the lack of shared security standards in the CAV domain and the increase of potential attack surface caused by the interconnection of different CAV components.[10]

On the other hand, while European data protection legislation such as the GDPR, ePrivacy and NISD provide a minimum level of legal safeguards for citizens, they may not suffice to maximize CAV benefits for users while minimizing their potential negative impact on society.[11] In order to properly and comprehensively address the risks brought about by CAVs, ethics[12] and human rights concerns must therefore take a central role in every stage of the CAV development lifecycle, embedding the notions of fairness, transparency, and security into design processes. Transparency[13] is situated between the legal and ethical dimensions and is challenged by the complexity of AI systems, as well as the inherent autonomy and flexibility of automated decision-making, and is key in the development of the framework as a prerequisite for trustworthy, ethical, and fair data processing.

This paper explores the closely linked legal principles and ethical aspects that should be taken into consideration by stakeholders in the CAV landscape and provides a roadmap to be used by CAV researchers, developers, and all those who seek to create and implement technologies to carry out data processing activities within such domain in a compliant, fair and trustworthy manner. As a result of the inherent link between the legal and ethical concerns, the authors will present a holistic approach to design and development which is intended to overcome the challenges posed to European personal data protection legal principles and obligations, by involving ethics and fairness. This approach, which goes beyond minimum legal requirements and proposes the application of a multidisciplinary framework, can be defined as Data Protection as a Corporate Social Responsibility in accordance to the Maastricht methodology in this domain.[14]

KEYWORDS

Artificial Intelligence, Data Protection, Corporate Social Responsibility, Connected and Automated Vehicles

1 INTRODUCTION

Emerging technologies and tools based on Artificial Intelligence (AI), such as Connected and automated vehicles (CAV or CAVs), present novel regulatory and legal compliance challenges while at the same time raising important questions with respect to ethics and transparency. CAVs bring to light theoretical and practical challenges to the implementation of the multi-dimensional obligations of the General Data Protection Regulation (GDPR), the ePrivacy directive[15] (2002/58/EC, revised by 2009/136/EC) and, where applicable, the Directive for a high common level of security and information systems (NIS Directive or NISD).[16] Though briefly

[8] See Article 7(3) GDPR.

[9] The risk-based approach is promoted by the GDPR, which encourages organizations to evaluate the risks inherent in the processing activities and to then implement a framework to mitigate such risks.

[10] See European Data Protection Supervisor, *Connected Cars*, TechDispatch, Issue 3, 20 December 2019, p. 2. Available at: https://edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-3-connected-cars_en; and the European Union Agency for Cybersecurity, *Good Practices for Security of Smart Cars*, 25 November 2019, pp. 6-7. Available at: https://www.enisa.europa.eu/publications/smart-cars.

[11] European Data Protection Board, *Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications*, Version 1.0, 28 January 2020, p. 10. Available at: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf.

[12] Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659). *Ethics of Connected and Automated Vehicles: recommendations on road safety, privacy, fairness, explainability and responsibility.* 2020. Publication Office of the European Union: Luxembourg. Available at: https://ec.europa.eu/info/sites/info/files/research_and_innovation/ethics_of_connected_and_automated_vehicles_report.pdf.

[13] Articles 13 and 14 GDPR require controllers to provide clear information to data subjects when their personal data is being obtained from them, including, e.g., information on the identity and contact details of the controller, the purposes of the processing, the categories, recipients and storage of personal data.

[14] The concept of Data Protection as a Corporate Social Responsibility (DPCSR) has been developed and promoted by Prof. Dr. Paolo Balboni (Maastricht University), after having launched the idea on his blog in 2017. The Maastricht University DPCSR project (Maastricht DPCSR or MU DPCSR) of the European Centre on Privacy and Cybersecurity (ECPC) at Maastricht University is a two-year multi-stakeholder research project that commenced in January 2020 and involves both Data Protection and Business Stakeholders. During the first year of the project the researchers have concretized three rules for each of the Five Principles of Sustainable Data Protection previously identified by Dr. Paolo Balboni and explored during his inaugural lecture. The second year of the project will consist of expanding to five rules per principle, for a total of 25 rules, which will form the basis of the Maastricht DPCSR Framework. The first manifesto of the project detailing the aforementioned principles and rules, "Data Protection as a Corporate Social Responsibility: From Compliance to Sustainability to Generate Both Social and Financial Value", is available here: https://www.maastrichtuniversity.nl/ecpc/csr-project/csr-publications. The research project is being developed according to the highest academic and ethical standards in full independence. It is intended to benefit of the rights and freedoms of individuals by way of the establishment of data protection practices that are socially responsible and feasible, and which shall be agreed upon and adhered to by the Stakeholders. The Maastricht DPCSR Framework aims to "trigger virtuous data protection competition between companies by creating an environment that identifies and promotes data protection as an asset which can be used to help companies to responsibly further their economic targets." To learn more about the project, see the University's dedicated webpage, available here: https://www.maastrichtuniversity.nl/ecpc/csr-project.

[15] The ePrivacy Directive "sets a specific standard for all actors that wish to store or access information stored in the terminal equipment of a subscriber or user in the European Economic Area (EEA)." The majority of the provisions in the ePrivacy Directive (e.g. Articles 6 and 9) only apply "to providers of publicly available electronic communication services and providers of public communication networks, art. 5(3) ePrivacy Directive is a general provision. It does not only apply to electronic communication services but also to every entity that places on or reads information from a terminal equipment without regard to the nature of the data being stored or accessed." See p. 5 of the European Data Protection Board *Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications*, Version 1.0, 28 January 2020. Available at: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf.

Also note that according to Art. 1(a) of Directive 2008/63/EC, terminal equipment is defined as "equipment directly or indirectly connected to the interface of a public telecommunications network to send, process or receive information; in either case (direct or indirect), the connection may be made by wire, optical fibre or electromagnetically; a connection is indirect if equipment is placed between the terminal and the interface of the network; (b) satellite earth station equipment". See the Directive here: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32008L0063. Following this logic, the European Data Protection Board has determined that "the connected vehicle and every device connected to it shall be considered as a 'terminal equipment' (just like a computer, a smartphone or a smart TV) and provisions of art. 5(3) ePrivacy Directive must apply where relevant." See European Data Protection Board *Guidelines 1/2020*, p. 5.

[16] The NISD, applicable to *operators of essential services* and *digital service providers,* ensures the security of network and information systems vital to economic and societal activities and to the functioning of the internal EU market. Also see Recital (1) NISD.

touching on other legislation, this paper will primarily deal with requirements enshrined in the GDPR.

In the context of CAVs, adherence to the rules set forth in the GDPR is fundamental for conformity with the applicable legal framework,[17] which establishes compliance requirements for entities that process personal data, or information relating to individuals which can be either identified or identifiable.[18] Consequently, when designing and developing CAVs, it is crucial to have an overview of the difficulties that arise as a result of the implementation of the GDPR, and to have an approach to adequately address them. Furthermore, the ePrivacy Directive is also directly relevant to CAVs in that it specifies standards for the storage of and access to information stored in "terminal equipment of a subscriber or user"[19] in the European Economic Area, notably imposing the need to collect specific GDPR-compliant consent[20] from CAV users for these activities. This particular requirement, as seen previously, may generate technical and legal difficulties for certain subsequent uses of information gathered from CAVs. The NIS Directive instead has established further obligations to ensure the security of network and information systems of essential services of a given Member State, classified as "*operators of essential services*" (such as telecommunications, healthcare or transportation services). The European Union Agency for Cybersecurity (ENISA) has identified intelligent transport systems (ITS) as Essential Service Operators in the road transport sub-sector,[21] and therefore it can be concluded that the NISD is applicable also in the context of CAVs. At the moment ENISA is in the process of addressing the security of smart cars in order to contribute to the existing regulatory framework. It is therefore safe to assume that as the adoption of CAVs reaches a critical mass, that specific ITS operators will be designated as operators of essential services.

As mere examples, CAV manufacturers, including vehicle and equipment manufacturers, developers, service providers and other relevant third parties (also collectively referred to as "CAV stakeholders") currently face multiple legal hurdles to overcome, including the necessity to fulfil controller and/or processor obligations in complex data processing scenarios[22] and tensions with the GDPR's principle of purpose limitation[23] (which comes at odds with the CAV's autonomous processing of personal data through AI, which may be based on a (re)interpretation of goals, or, possibly, a shift in focus from the original goal for which personal data was collected).[24] Additionally, the overall need for relatively large datasets to properly train and leverage AI functionalities leads to conflict with the principle of data minimization.[25] When applied to AI systems, data protection by design and by default also presents difficulties, as data protection by default is possible only when the necessary personal data is processed for a specific purpose.[26] Concerns from the data security[27] perspective are also highly relevant, notably due to the lack of shared security standards in the CAV domain and the increase of potential attack surface caused by the interconnection of different CAV components.[28]

At the same time, while European data protection legislation such as the GDPR provides a minimum level of legal safeguards for citizens, they may not suffice to maximize CAV benefits for users while minimizing their potential negative impact on society.[29] In order to properly and comprehensively address the risks brought about by CAVs, ethics and human rights concerns must therefore take a central role in every stage of the CAV development lifecycle, embedding the notions of fairness, transparency, and security into design processes. Transparency[30] is situated between the legal and ethical dimensions and is challenged by the complexity of AI systems, as well as the inherent autonomy and flexibility of automated decision-making, and is key in the development of the

[17] European Data Protection Board, *Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications*, Version 1.0, Adopted on 28 January 2020, p. 5.

[18] Under Art. 4(1) GDPR, data subject is defined as "*an identified or identifiable natural person*". Please see footnote 55 for the explanation provided by the GDPR of an "identifiable natural person". Also see a recent landmark case of the Court of Justice of the European Union which clarifies that the concept of personal data is to be extended to cases where even only a third party has additional data necessary to identify the data subject (Case C-582/14, Patrick Breyer v Bundesrepublik Deutschland). Available at: http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1116945.

[19] See Article 5(3) ePrivacy Directive.

[20] See Recital 17 ePrivacy Directive which, with the entering into force of the GDPR, should be read as referring to the GDPR's requirements on consent (and not those of its predecessor, Directive 95/46/EC).

[21] "In light of the NIS Directive, in which road authorities and intelligent transport systems are among the entities identified as Essential Service Operators in the road transport sub-sector, there is a growing need for addressing the security of smart cars." See European Union Agency for Cybersecurity, *ENISA Programming Document 2020-2022,* November 2019, p. 32. Available at: https://www.enisa.europa.eu/publications/corporate-documents/enisa-programming-document-202020132022.

[22] Under the GDPR, there are two main roles that an organization can take on regarding an activity which involves the processing of personal data: that of controller, or that of processor. Article 4 (7) GDPR defines controller as "*the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data*"; where two or more controllers jointly determine the purposes and means of a given processing activity, they will be considered as "*joint controllers*" under Article 26 GDPR. Article 4 (8) GDPR defines processor as "*a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*". Depending on the data protection role which is applicable to an organization, its obligations will change, as can be better seen in Articles 25 to 28. Also see European Data Protection Board, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, Version 1.0, Adopted on 2 September 2020. Available at: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en.

[23] According to Article 5(1)(b) GDPR, personal data must be "*collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes*". Also see Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation*, 2 April 2013. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

[24] European Commission, *White Paper on Artificial Intelligence – A European approach to excellence and trust*, February 2020, p. 17. Available at: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf, p. 16.

[25] The principle of data minimization requires that personal data is to be processed to the extent to which it is "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*", according to Article 5(1)(c) GDPR. See European Data Protection Board, *Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications*, Version 1.0, 28 January 2020, p. 14. Available at: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf.

[26] Commission Nationale Informatique & Libertes, *Compliance Package: Connected vehicles and personal data.* October 2017. Available at: https://www.cnil.fr/sites/default/files/atoms/files/cnil_pack_vehicules_connectes_gb.pdf

[27] The risk-based approach is promoted by the GDPR, which encourages organizations to evaluate the risks inherent in the processing activities and to then implement a framework to mitigate such risks.

[28] European Union Agency for Cybersecurity, *Good Practices for Security of Smart Cars*, November 2019, pp. 6-7.

[29] European Data Protection Supervisor, *Report Towards a digital ethics – EDPS Ethics Advisory Group*, 25 January 2018. Available at: https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf.

[30] Articles 13 and 14 GDPR require controllers to provide clear information to data subjects when their personal data is obtained from them, including, e.g., information on the identity and contact details of the controller, the purposes of the processing, the categories, recipients and storage of personal data.

framework as a prerequisite for trustworthy, ethical, and fair data processing.

This paper explores the closely linked legal principles and ethical aspects that should be taken into consideration by stakeholders in the CAV landscape and provides a roadmap to be used by CAV researchers, developers, and all those who seek to create and implement technologies to process personal data within such domain in a compliant, fair and trustworthy manner. The protection of the rights, freedoms and interests of data subjects is at the heart of this discussion, though the perspective of technology service developers and providers – who carry the burden of implementing measures to ensure compliance with the existing legal framework – are addressed.[31] On the basis of the analysis laid out in this paper, we provide suggestions and recommendations in order to assist manufacturers, developers and service providers to design and develop CAVs. In fact, the adoption of a holistic approach to data protection can assist in overcoming both the ethical and legislative and regulatory challenges in this complex environment. This approach, which goes beyond minimum legal requirements and proposes the application of a multidisciplinary framework, can be defined as Data Protection as a Corporate Social Responsibility in accordance to the Maastricht methodology in this domain.[32]

2 PRIMARY LEGAL AND ETHICAL CONCERNS IN THE CAV ENVIRONMENT

The automotive industry of the 21st century has transformed traditional cars into intelligent objects of transportation.[33] The technology of Connected and Automated Vehicles cannot be separated from the persons that use them, whether for their private use or as part of services of a public system of transportation. It cannot be denied that the human-machine relationship, the human to the CAV, itself presents a number of ethical paradoxes and concerns which range from safety and even the loss of human life, liability questions, to economic, environmental, and security, privacy and data protection concerns.[34] Furthermore, the absence of a specific applicable legislative framework and appropriate consideration of the ethical implications of such new technologies presents a challenge both for manufacturers in the development and steering of their work and to society with respect to the benefits that can be reaped from such technologies, whether they be increased road safety, lessened environmental impact and better mobility, or the potential improvement of European economic strength, growth, and competitiveness.[35] As is often the case with new technologies, which make rapid and significant progress in terms of development and adoption, policymaking and the applicable regulatory frameworks are often less less-advanced than the technology itself, a notion which also holds true in the area of CAVs.[36] This, together with the fact that such new technologies present both significant opportunities, but also risks, underlines the necessity of adequate regulation.[37]

CAVs operate in a complex communications ecosystem whose interactions can largely be divided into vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-everything (V2E or V2X),[38] involving actors that range from the driver, passenger, pedestrian, to smart city infrastructure managers, law enforcement, and infotainment service providers.[39] Connected vehicles furthermore include numerous additional characteristics and innovative technologies, and entail the constant processing of (personal) data for the improvement of driving, requiring the transmission of data relating to the car, its surroundings and the individuals inside it.[40] Connected vehicles largely function by collecting various types of information, depending on their design, through built-in or external sensors (e.g., external devices, such as a smartphone). Autonomous vehicles use such sensors and AI in order to autonomously perform driving functions under varied conditions.[41] The inherent nature of CAVs therefore involves the collection of massive amounts of data, for an uncertain number of purposes (which may not be disclosed from the start of the use of the CAV) and the security includes a

[31] Also see Recital 78 GDPR.

[32] The concept of Data Protection as a Corporate Social Responsibility (DPCSR) has been developed and promoted by Prof. Dr. Paolo Balboni (Maastricht University), after having launched the idea on his blog in 2017. The Maastricht University DPCSR project (Maastricht DPCSR or MU DPCSR) of the European Centre on Privacy and Cybersecurity (ECPC) at Maastricht University is a two-year multi-stakeholder research project that commenced in January 2020 and involves both Data Protection and Business Stakeholders. During the first year of the project the researchers have concretized three rules for each of the Five Principles of Sustainable Data Protection previously identified by Dr. Paolo Balboni and explored during his inaugural lecture. The second year of the project will consist of expanding to five rules per principle, for a total of 25 rules, which will form the basis of the Maastricht DPCSR Framework. The first manifesto of the project detailing the aforementioned principles and rules, "Data Protection as a Corporate Social Responsibility: From Compliance to Sustainability to Generate Both Social and Financial Value", is available here: https://www.maastrichtuniversity.nl/ecpc/csr-project/csr-publications. The research project is being developed according to the highest academic and ethical standards in full independence. It is intended to benefit of the rights and freedoms of individuals by way of the establishment of data protection practices that are socially responsible and feasible, and which shall be agreed upon and adhered to by the Stakeholders. The Maastricht DPCSR Framework aims to "trigger virtuous data protection competition between companies by creating an environment that identifies and promotes data protection as an asset which can be used to help companies to responsibly further their economic targets." To learn more about the project, see the University's dedicated webpage, available here: https://www.maastrichtuniversity.nl/ecpc/csr-project.

[33] European Union Agency for Cybersecurity, *Good Practices for Security of Smart Cars*, November 2019, p. 7.

[34] German Federal Ministry of Transport and Digital Infrastructure, *Ethics Commission Automated and Connected Driving*. June 2017. Available at: https://www.bmvi.de/SharedDocs/EN/publications/report-ethics-commission.pdf?__blob=publicationFile. Also see European Parliamentary Research Service, Study of the Panel for the Future of Science and Technology, *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence.* June 2020. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf; and ICT Legal Consulting's contribution to nIoVe Deliverable 2.1. https://niove.eu/.

[35] Government of The Netherlands, *Self-driving cars,* 2020. https://www.government.nl/topics/mobility-public-transport-and-road-safety/self-driving-vehicles.

[36] This concept is furthered in the June 2018 report of the Task Force on Ethical Aspects of Connected and Automated Driving (Ethics Task Force) established by the 2nd High Level Structural Dialogue in Frankfurt/M. on 14 and 15 September 2017. Available at: https://www.bmvi.de/SharedDocs/EN/publications/report-ethics-task-force-automated-driving.pdf?__blob=publicationFile.

[37] European Commission, *White Paper on Artificial Intelligence – A European approach to excellence and trust*, European Commission, February 2020, pp. 3, 17. Available at: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

[38] WSP Canada Group Limited and Ontario Centres of Excellence, *Ontario CAV Ecosystem Analysis*, 2019, p. 4. Available at: https://www.oce-ontario.org/docs/default-source/publications/avin-ecosystem-analysis-final-report-2019.pdf?sfvrsn=2.

[39] European Data Protection Board, *Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications*, Version 1.0, 28 January 2020, p. 3.

[40] European Data Protection Supervisor, *Connected Cars*, TechDispatch, Issue 3, 2019, p. 1.

[41] European Union Agency for Cybersecurity, *Good Practices for Security of Smart Cars*, November 2019, p. 13.

considerably large ecosystem of devices (both internal and external to the CAV).[42] For such reasons, CAVs have introduced novel regulatory and legal compliance challenges[43] which remain to be fully addressed by policymakers.[44]

Current legislation governing the processing of personal data[45] related to individuals, those who drive or ride in CAVs, is the General Data Protection Regulation (GDPR)[46] which applies to "the processing of personal data wholly or partly by automated means"[47] and the ePrivacy Directive, which creates specific consent requirements applicable to the storage of, and access to, information stored in CAVs.[48] Data subjects are afforded a variety of rights under the GDPR, which also establishes important principles – this also applies to CAV manufacturers, service developers/providers and users, where such services require the use of personal data. As such, compliance with the principles of the GDPR relating to the processing of personal data, including the principles of lawfulness, fairness and transparency,[49] purpose limitation,[50] data minimisation, accuracy, storage limitation, the principles of integrity and confidentiality (data security) and the principle of accountability[51] are required.

2.1 Data Processing Scenarios and Data Processing Roles

An initial hurdle in the development of CAVs is the fact that the processing of personal data is often carried out by machines managed by different organisations, each of them using computational capacity provided by cloud service developers/providers and that can also involve analytic software programmes supplied by the related vendors.[52] This exponentially increases the number of parties involved in data processing activities and the difficulties in clearly allocating data processing roles (controller or processor) to each one. Such grey areas create both compliance and ethical complications[53] with respect to accountability where stakeholders feel that the responsibility for data protection compliance lies with another entity, and thus may feel free to process personal data in ways that they deem more convenient or beneficial, perhaps to the detriment of the individuals concerned.

Under the GDPR, when processing personal data, there are two main roles that an organization can take on, that of the data controller and that of the data processor. The data controller is the party that determines the purposes (the why) and the means (the what and how) of the processing.[54] For example, service providers that process vehicle data to send the driver messages, insurance companies or vehicle manufacturers, tend to take the role of a data controller, since they collect data on vehicle use and for their own purposes (i.e., service provision and quality improvement).[55] In this category, two or more data controllers may also jointly determine the purposes and means of the processing, and they will be considered as joint controllers.[56] The data processor is the entity which

[42] European Data Protection Board, *Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications*, Version 1.0, 28 January 2020, p. 14. Available at: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf.

[43] The Article 29 Data Protection Working Party in its *Opinion 08/2014 on the Recent Developments on the Internet of Things* (16 September 2014) has linked IoT to the notions of "pervasive" and "ubiquitous" computing, thereby "*clearly [raising] new and significant personal data protection and privacy challenges*".

[44] European Union Agency for Cybersecurity, *Towards a framework for policy development in cybersecurity, security and privacy considerations in autonomous agents*, 14 March 2019, p. 17. Available at: https://www.enisa.europa.eu/publications/considerations-in-autonomous-agents.

[45] Article 4(1) of 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 (available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj) defines personal data as "*any information relating to an identified or identifiable natural person*", further specifying that "*an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*". Article 4(2) of the same Regulation defines *processing* as "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*".

[46] 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. Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

Manufacturers, and service developers/providers may further be subjected to rules arising from the European Union's Directive on Security of Network and Information Systems (NISD), depending on the types of services they provide. In particular, when involved in the provision of crucial services for the functioning of a given Member State, such as telecommunications, healthcare or transportation services, these developers/providers may be classified as "operators of essential services" (OESs). (See 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. Available at: https://eur-lex.europa.eu/eli/dir/2016/1148/oj, and Arts. 4(4) and 5(2), as well as Annex II NISD.) These operators are subject to further obligations under the NISD, intended to promote and ensure the security of network and information systems deemed vital to economic and societal activities, and in particular to the functioning of the European Union's internal market. (Recital (1) NISD).

[47] Article 2(1) General Data Protection Regulation.

[48] See Article 5(3) ePrivacy Directive and European Data Protection Board, *Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications, Version 1.0, 28 January 2020,* Section 1.2. Available at: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf.

[49] Article 29 Working Party, *Guidelines on transparency under Regulation 2016/679*, 29 November 2017, as last Revised and Adopted on 11 April 2018. Available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

[50] Article 29 Working Party, *Opinion 03/2013 on purpose limitation*, 2 April 2013. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

[51] Article 29 Working Party, *Opinion 03/2010 on the principle of accountability*, 13 July 2010. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf.

[52] Article 29 Data Protection Working Party, *Opinion 8/2014 on Recent Developments on the Internet of Things*, 16 September 2014, p. 11. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf. See also European Data Protection Supervisor, *EDPS response to the Commission public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy*, 16 December 2015, p. 4. Available at: https://edps.europa.eu/sites/edp/files/publication/15-12-16_online_platforms_en.pdf.

[53] According to the "a broader and more proactive ethical approach will also help to reveal new perspectives on the often-asked question of who is responsible for the behaviour of CAVs." See Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659). *Ethics of Connected and Automated Vehicles: recommendations on road safety, privacy, fairness, explainability and responsibility.* 2020. Publication Office of the European Union: Luxembourg, p. 20. Available at: https://ec.europa.eu/info/sites/info/files/research_and_innovation/ethics_of_connected_and_automated_vehicles_report.pdf.

[54] Article 4(7) General Data Protection Regulation.

[55] European Data Protection Board, *Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications*, Version 1.0, 28 January 2020, p. 9.

[56] On the concept of joint controllers, see European Data Protection Board, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, Version 1.0, Adopted on 2 September 2020; also see relevant Court of Justice of

processes personal data on behalf of the controller, based on the instructions of the controller.[57] Suppliers and equipment manufacturers who may process data on behalf of CAV manufacturers may be processors in this context.[58]

The European Commission has clarified that the principle of accountability lies with the actor(s) best placed to address risks.[59] Therefore, the criteria[60] of who is in the best position to address risks can help CAV manufacturers, service providers, and developers take the appropriate data processing role in the different stages of the lifecycle (i.e., developers, users and third parties will therefore be responsible at different stages of the lifecycle). According to Art. 28(3) GDPR, controllers must regulate their relationship with processors through a contractual agreement, which is inconsistent with the reality that the same actors can have different data processing roles depending on the stage of the lifecycle.

More conventional agreements to regulate data processing relationships, such as Data Processing Agreements[61] and joint controllership agreements[62] may prove impractical to deal with these intricate relationships, as they may not suffice to cover all different roles which each of the parties involved in CAV data processing plays. In order to address the grey area and the need to sign several Data Processing Agreements, stakeholders should consider engaging each other through more complex contractual frameworks (Data Management Agreements[63]), identifying the specific CAV data processing activities which they intend to perform and their respective roles and obligations for each activity identified.[64] In this respect, a level playing field for CAV-collected and shared data can create greater certainty between the actors and greater assurances for lawful processing towards data subjects.

2.2 Data Protection by Design and by Default

Adherence to the concept of data protection by design and by default[65] represents a fundamental prerequisite in the design of CAV, requiring controllers from the design phase to implement technical and organisational measures within products and services to ensure compliance with the GDPR and the protection of data subjects' rights, "*both at the time of the determination of the means for processing and at the time of the processing itself*" (data protection by design[66]). Data protection by design and by default should not simply be considered as a principle, but rather, as a means to achieve compliance with the specific principles stipulated in Article 5 GDPR, and generally, all duties and obligations set forth in the GDPR. Art. 25(2) GDPR more specifically requires the implementation of measures to make the principle of data minimisation effective, by only allowing the processing of personal data which is strictly necessary for the processing purposes which have been identified for a given activity (data protection by default[67]). In order to apply data protection by design and by default, organizations should first develop of a comprehensive risk assessment, where the intended activity is mapped out from the personal data perspective.[68] Additionally, according to the principle of integrity and confidentiality, personal data must be processed in a manner that ensures appropriate security of the personal data, including the protection against unauthorised or unlawful and against accidental

the European Union Case C-210/16 (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH). Available at: http://curia.europa.eu/juris/document/document.jsf?text=&docid=202543&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1206721; Case C-25/17 (Tietosuojavaltuutettu v Jehovan todistajat). Available at: http://curia.europa.eu/juris/document/document.jsf?docid=203822&doclang=EN; and Case C-40/17 (Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV), which concerns the joint controllership relationship between Facebook and website operators that embed the Facebook "Like" button on their site. Available at: http://curia.europa.eu/juris/liste.jsf?num=C-40/17.

[57] Article 4(8) General Data Protection Regulation.

[58] European Data Protection Board, *Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications*, Version 1.0, 28 January 2020, p. 9.

[59] European Commission*, White Paper on Artificial Intelligence – A European approach to excellence and trust*, February 2020, p. 22. Available at: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

[60] European Data Protection Board, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR,* Version 1.0, 2 September 2020. Available at: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en.

[61] Agreements entered into between a controller and a processor, to regulate the processor's processing of personal data on behalf of the controller, meeting the minimum requirements of Art. 28 GDPR.

[62] Agreements entered into between joint controllers, to regulate their respective data protection responsibilities under the GDPR in a consistent and transparent manner, meeting the minimum requirements of Art. 26 GDPR.

[63] Multi-part structured agreements which include terms applicable to controller-to-processor, joint controllership and independent controllership relationships and identify the scenarios in which each relevant party will be bound by each set of terms.

[64] This builds upon the recommendation made by the European Data Protection Supervisor in its *EDPS response to the Commission public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy*, 16 December 2015, p. 5. Available at: https://edps.europa.eu/sites/edp/files/publication/15-12-16_online_platforms_en.pdf: "The most effective regulatory response, in the above respect, consists of applying in a coherent way the Data Protection Directive, which identifies the controller as 'the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data' and assigns to it the fulfilment of a number of duties designed to protect the individual's rights to privacy and data protection. Therefore, before engaging into any data processing, platform operators and other service providers should identify themselves as data controllers (or [joint controllers]) in the information they provide to users whose data they process. They can identify their position as controllers based on the mere fact that they are processing personal data for their own purposes. This approach ensures that businesses act responsibly and in compliance with the Directive and that liability is efficiently allocated".

[65] For more information on the concept of data protection by design and by default, please see the United Kingdom Information Commissioner's checklist, available here: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/; the Spanish Data Protection Authority's (AEPD) Guidelines on Data Protection by Default – *"Guía de Protección de Datos por Defecto"* (October 2020), available here: https://www.aepd.es/sites/default/files/2020-10/guia-proteccion-datos-por-defecto.pdf; and the AEPD's Guidelines on Privacy by design - *"Guía de Privacidad desde el Diseño"* (October 2019), available here: https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-desde-diseno.pdf.

[66] As noted by the European Data Protection Supervisor in his *Opinion 5/2018 – Preliminary Opinion on privacy by design* (31 May 2018, available at: https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf), the obligation of data protection by design, under Art. 25 GDPR, can be broken down into 4 dimensions: (1) personal data processing should always be the outcome of a design project; (2) a risk management approach must be followed in the selection and implementation of measures for effective protection; (3) measures selected must be appropriate and effective; and (4) the identified measures/safeguards must be integrated into the processing activity itself.

[67] In particular, as noted by Art. 25(2) GDPR, this obligation "*applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility*", and measures taken to address this obligation "*shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.*"

[68] On this, see European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default,* 13 November 2019. Available at: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf. In particular, see pp. 13 *et seq.* which provide a checklist which organisations can use to measure their level of implementation of each Art. 5 GDPR principle.

loss, destruction or damage, using appropriate technical or organisational measures.[69]

The European Commission has established that AI applications should be considered high-risk if the application is employed in a sector where significant risks for individuals can be expected, including the transportation sector.[70] Thus, CAV designing should initiate by carrying out a Data Protection Impact Assessment (DPIA), which would acknowledge and assess the risks posed to data subjects. DPIAs should be complemented with extensive Security Risk Assessments in order to identify threats and risks on IT systems and assess whether security measures in place provide an adequate level of protection, also taking into account the magnitude and seriousness of the security risks increase with the large attack surface. This integrated approach can be found in the Maastricht DPCSR principle of Data security by design,[71] which calls for the implementation of a risk-based approach to data processing that aids in the management of data security in order to optimize economic and social benefits of product deployment and use. Such an approach to data security is necessary in order for society to take full advantage and benefit from technological advancements in transportation in the CAV context, by first successfully mitigating the risks posed by such technologies in terms of security.[72]

The described regime of Data security by design leads to the obligation of developers and manufacturers to have a good approach to security based to an analysis of the risks associated to individuals involved, namely drivers, passengers, and pedestrians. The mitigations envisioned for such risks should be transposed into documented policies and procedures, also in view of a comprehensive *future* risk analysis that is aimed at identifying threats that may pose risks to CAV systems. It essentially calls for CAVs to be safe by design, taking into account "known patterns of use by CAV users, including deliberate or inadvertent misuse, as well as tendencies toward inattention, fatigue and cognitive over/under-load."[73]

Solutions for mitigating the high risks relating to CAVs should include human oversight, the adoption of an Ethics by design and User empowerment by design approach,[74] and the monitoring of the AI system.[75] Human oversight should ensure the ability for humans to intervene in real time through deactivation during operation, for example, a stop button or a procedure when a human determines that car operation is not safe.[76] In the designing of the CAV, operational constraints can be implemented, for example for the CAV to stop operating in critical weather conditions. Furthermore, a supervision centre should interact with the vehicle to monitor its status, request actions and perform remote administration tasks.[77] The ethical question of connected and autonomous vehicles, in fact, is also dependent on "the conditions in which they are used and the way in which they are designed,"[78] solidifying the relationship between the legal prescription and the ethical aspects of CAVs.

2.3 Fairness by Design

Following the logic of data protection by design and default, in the development process of CAVs, car manufacturers and relevant technology providers should closely enforce the concept of "fairness by design" by which fairness is related to balanced and proportionate data processing.[79] Fairness by design requires the balancing of fundamental rights freedoms, which should be built into the very design of connected vehicles, their components, and more generally, all the related data processing activities in the CAV environment, forming an integral part of the algorithms that underpin the related processing activities. In this way, Fairness by design acts as a further specification of the concept of data protection by design, complementing both the legal and the ethical dimensions

[69] Art. 5(1)(f) GDPR. For more information on the principle of security, see, e.g., the United Kingdom Information Commissioner's Office, *Security*, available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/.

[70] European Commission, *White Paper on Artificial Intelligence – A European approach to excellence and trust*, February 2020, p. 17. Available at: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

[71] See Maastricht DPCSR *Principle 1, Rule 1: Implement Data Security by Design. The Organization shall implement Data Security by Design into its data processing activities.* Available at: https://www.maastrichtuniversity.nl/ecpc/csr-project/csr-publications.

[72] In the context of CAVs, which make use of Artificial Intelligence, the security of the algorithm is of fundamental concern, also to protect human life, where malicious actors could take control of vehicles or slowly divert algorithms to go off course or even intentionally cause accidents. According to ENISA, specific risks from attacks may include, "vehicle immobilization, road accidents, financial losses, disclosure of sensitive and/or personal data, and even endanger road users' safety. Thus, appropriate security measures need to be implemented to mitigate the potential risks, especially as these attacks threaten the security, safety and even the privacy of vehicle passengers and all other road users, including pedestrians." See *ENISA Good practices for security of Smart Cars*, 25 November 2019, p. 5. Available at: https://www.enisa.europa.eu/publications/smart-cars.

[73] Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659*). Ethics of Connected and Automated Vehicles: recommendations on road safety, privacy, fairness, explainability and responsibility.* 2020. Publication Office of the European Union: Luxembourg, p. 8. Available at: https://ec.europa.eu/info/sites/info/files/research_and_innovation/ethics_of_connected_and_automated_vehicles_report.pdf.

[74] Maastricht DPCSR *Principle 1, Rule 2: Implement Ethics by design and User Empowerment by design, actively empowering individuals with respect to their data*, calls for organizations to 1) establish a multi-stakeholder ethics and user empowerment board led by the person(s) charged with ensuring compliance with the Maastricht DPCSR Framework and involving the C-suite, researchers and developers/engineers, legal and marketing functions, as well as others deemed to be relevant by the organization; 2) Establish an internal-external multi-stakeholder ethics, user empowerment, accessibility, and functionality group which, through testing procedures and protocols and the inclusion of individuals outside of the organization including, e.g. users, ethicists, consumer and professional associations, disability rights activists, and other relevant stakeholders, can ensure that the objectives of the established procedures and protocols concerning ethics and user empowerment are met. 3) Develop personalized ethics and user empowerment by design policies and procedures (testing and verification protocols/ impact assessments), including ethics and user empowerment impact assessments which ensure that the objectives of the procedures and protocols with respect to ethics by design and user empowerment by design are met.

[75] *Principle 3, Rule 3* of the Maastricht DPCSR framework, calls for organizations to "Establish trusted data processing activities (for example, for use in AI and big data analytics) that actively oppose bias and discrimination. The Organization shall actively seek not only to not cause harm, but to oppose bias and discrimination" to this end provides focuses on establishing trusted data processing activities that actively oppose bias and discrimination, and requires having in place checks and balances to prevent bias and discrimination in all levels of data processing activities, with specific reference to AI and algorithms. It is closely related to the concept of F*airness by design* (*Principle 1, Rule* 3) and can also implicate data sharing, which is further explored in *Principle 4, Publish relevant findings based on statistical/anonymized data to improve society.* Available at: https://www.maastrichtuniversity.nl/ecpc/csr-project/csr-publications.

[76] European Commission, *White Paper on Artificial Intelligence – A European approach to excellence and trust*, February 2020, p. 21. Available at: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

[77] Ibid.

[78] German Federal Ministry of Transport and Digital Infrastructure, *Ethics Commission Automated and Connected Driving.* June 2017, p. 6. Available at: https://www.bmvi.de/SharedDocs/EN/publications/report-ethics-commission.pdf?__blob=publicationFile.

[79] See Paolo Balboni, "The Automated Vehicle Consortium and Fairness by Design", May 2019. Available at: https://www.paolobalboni.eu/index.php/2019/05/08/the-automated-vehicle-safety-consortium-and-fairness-by-design/. Also see ICT Legal Consulting's contribution to nIoVe Deliverable 2.1.

of privacy and personal data protection for the development of a healthy and democratic digitalized society.

In line with this principle, developers and manufacturers should take into account the interests and reasonable expectations of privacy of data subjects from the design phase of the CAV. The processing of personal data in CAVs should not unreasonably intrude on the privacy, autonomy and integrity of data subjects nor pressure data subjects to provide their personal data, collecting only what is strictly necessary for the operation of the vehicle. Fairness by Design[80] leverages the highly relevant[81] principle of fairness embedded in Article 5(1)(a) GDPR, aiming to both regulate and to prevent any harm which may arise as a consequence of algorithmic processing of the CAV.

On the part of manufacturers and developers, the implementation of Fairness by design can be realized by way of integration of five recommendations into the CAV lifecycle. These include carrying out: 1) Human rights impact assessments;[82] 2) drawing red lines for certain types of processing that due to their nature represent too high of a threat to human rights and risk posing a severe and irreversible impact on fundamental rights and societal welfare in general; 3) providing for reinforced transparency and the right to algorithmic explanation;[83] 4) the provision of effective redress mechanisms (procedural fairness and algorithmic due process);[84] and 5) ensuring independent oversight. By implementing the above requirements of Fairness by design as they are established in the Maastricht DPCSR framework, stakeholders in the CAV environment can actively seek to embed the seeds of fairness directly into the design of connected vehicles.

2.4 Principle of Purpose Limitation

The principle of purpose limitation states that the personal data must be collected for a specified, explicit and legitimate purposes, without further processing in a manner that is incompatible with those purposes.[85] As noted by the Article 29 Data Protection Working Party, "*any processing following collection, whether for the purposes initially specified or for any additional purposes, must be considered 'further processing' and must thus meet the requirement of compatibility.*"[86] This notion of compatibility includes a criteria to be assessed by a controller in order to establish if a further processing purpose is compatible with the initial purpose for data collection:[87] 1) whether there is any link between these purposes; 2) the context in which the personal data was collected; 3) the nature of the personal data in question; 4) the possible consequences of the intended further processing for data subjects; and 5) the existence of appropriate safeguards, such as encryption or pseudonymisation.[88] Based on a factual assessment of the initial purpose of data collection and the intended further purpose, controllers can theoretically arrive at a conclusion as to whether the further purpose is compatible with the initial one[89] – and therefore that it does not require an additional, specific legal basis to be identified for it – or is instead incompatible,[90] and must be supported by its own specific legal basis. As a result, organizations have an obligation to map the purposes for which they collect personal data, and avoid reuse, combination or repurposing of those data for incompatible purposes.[91]

[80] The Maastricht Data Protection as a Corporate Social Responsibility Working Group has established that Fairness by Design embodies *Principle 1, Rules 1* (*Data Security by Design*) and 2 (*Ethics by design and User Empowerment by design*) and integrates the legal dimension of the GDPR. ICTLC Senior Associate Davide Baldini has actively contributed to the definition of *Principle 1, Rule 3, Fairness by design* and its relative five requirements as they are described above. Together these three rules form the initial triad on which the Maastricht DPCSR Framework is built. Also see Paolo Balboni and Kate Francis, "Data Protection as a Corporate Social Responsibility: From Compliance to Sustainability to Generate Both Social and Financial Value." European Centre on Privacy and Cybersecurity (ECPC), Maastricht University Faculty of Law website. 27 October 2020. Available at: https://www.maastrichtuniversity.nl/ecpc/csr-project/csr-publications.

[81] Art. 8(2) of the Charter of Fundamental Rights of the European Union provides that "Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified."

[82] Organizations which make use of new technologies such as algorithms for processing personal data should be able to demonstrate that the data processing they are undertaking does not violate the fundamental rights or legitimate interests and expectations of data subjects. Where this may be the case, it should be established that any identified impact is adequately offset by an advancement in other rights and interests, where the "essence" of all fundamental rights involved is respected (see art. 52 par. 1 of the Charter). The Council of Europe recommends carrying out Human rights impact assessments (HRIAs) and they also form part of the European Commission legislative proposal for AI. Fundamental Rights Impact Assessments (FRIAs), on the other hand, have been suggested in the AI context by the European Commission's High-Level Expert Group on AI. In such assessments, the risks and potential impact on human rights implicit in the use of the AI are identified alongside the relevant mitigatory measures taken by the organization, which have to be documented and updated throughout the duration of the processing according to the principle of accountability.

[83] Algorithmic transparency, meaning the possibility for an individual to understand how and why a decision affecting them was made by an algorithm, is an essential prerequisite to guarantee fairness in the related data processing activity. Individuals who have been adversely affected by an automated process have the right to understand when a decision that impacts them was taken, also in order for them to challenge the decision. Article 13(2)(f) and 14(2)(g) GDPR explicitly mandates for data controllers who implement automatic decision-making systems referred to in Article 22 GDPR to provide "*meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject*".

[84] Players in the CAV environment should provide for easily accessible and transparent solutions to individuals for them to challenge the algorithmic decision. The functioning of the redress mechanism should be disclosed in advance, e.g., by means of the privacy policy or within an *ad hoc* information notice, and individuals who have been subject to the algorithmic decision should be presented with clear indications on how to make use of the designated redress mechanism made available by the organization.

[85] Art. 5(1)(b) GDPR. For more information on the principle of purpose limitation, see, e.g., the United Kingdom Information Commissioner's Office, *Principle (b): Purpose limitation*, available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/.

[86] Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation*, 2 April 2013, p. 21. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

[87] Note that Art. 6(4) GDPR generally allows further processing to take place, even in the absence of compatibility with the original processing purposes, where consent is relied on as a legal basis for the further processing, or where the further processing is authorised by Union or Member State law.

[88] Please note that the Article 29 Data Protection Working Party *Opinion 03/2013 on purpose limitation* refers to four steps, while the GDPR includes five steps. Nevertheless, substantially the steps are not changed.

[89] For example, by applying the compatibility test factors within the Data Protection Directive – Directive 95/46/EC – which are similar to those within Article 6(4) GDPR, the Article 29 Data Protection Working Party presented a scenario where a car manufacturer's further use of public vehicle registry data to notify car owners of malfunction and recall affected cars as compatible with the initial purpose for which those vehicle registry data were collected. See Example 11 of Annex 4 of Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation*, 2 April 2013. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

[90] As noted by the Article 29 Data Protection Working Party in their *Opinion 03/2013 on purpose limitation*, further processing of personal data for tracking and profiling for marketing purposes can usually only be considered as compatible if there is a lawful basis for the processing such as genuine, unambiguous, freely given and informed consent (see Example 10 of Annex 4).

[91] Purpose limitation and minimisation should "be interpreted in such a way that they do not exclude the use of personal data for machine learning purposes. They should not preclude the creation of training sets and the construction of algorithmic models,

While the compatibility test under Article 5(1)(b) and 6(4) GDPR appears, in theory, to potentially expand the possibilities under which collected CAV data may be re-used for subsequent purposes, there is a potential conflict between this test and the ePrivacy Directive's specific requirement for consent to be obtained from CAV users for the storage of, and access to, CAV information. Given this strict consent requirement, and the fact that GDPR-compliant consent must be *specific* (i.e., referring to a specific, explicit and legitimate processing purpose, to the exclusion of other purposes),[92] the EDPB has interpreted the GDPR's compatibility test as largely inapplicable to CAV data processing, with CAV stakeholders needing to seek additional consent (or otherwise, to identify an applicable legal obligation) to support any further processing of CAV data for subsequent purposes.[93]

This obligation comes at odds with the CAV's autonomous processing of personal data through AI, which may be based on a (re)interpretation of goals, or, possibly, a shift in focus from the original goal for which the personal data was collected. Even though this can pose several barriers in the use of personal data for other purposes, the flexible application of "compatibility" allows for the reuse of personal data, when it is not incompatible with the original purpose. Additionally, the CAV stakeholders can reuse the personal data for statistical purposes, unless it involves unacceptable risks for the data subject.[94]

2.5 Principle of Data Minimisation

The principle of data minimisation requires that personal data is processed in an adequate and relevant way, limited to what is necessary in relation to the purposes for which they processed.[95] This principle requires to only process the personal data which is strictly necessary for the purposes of the processing. The CAV collects a great deal of information as a result of the functions it offers, such as infotainment systems (e.g., seat entertainment), or through the telematics ecosystem (e.g., Global Navigation Satellite Systems data), and can exchange that data with any other entity (V2X communication), such as traffic signals, smart homes, or other vehicles.[96] The number of sensors, connected devices and network communications enhance the CAV stakeholders' possibility to collect and process personal data. It therefore becomes a tempting ecosystem for exploiting all plausible data collected by the CAV, at the risk of violating the rights and freedoms of data subjects. Further, the needs for relatively large datasets to properly train and leverage AI functionalities is problematic because it may be interpreted as a violation of the principle of data minimisation. However, there are numerous solutions that can be implemented in order to ensure that data minimisation is complied with.

The starting point of vehicle and equipment manufacturers, service providers and developers must be to have a clear overview of the categories of data they need from a CAV by utilising the two following criteria: 1) it should be relevant for the intended specific processing, 2) is it necessary for the intended specific processing.[97] Although this is a subjective test, all CAV stakeholders should aim to carry out this assessment prior to the collection of personal data and be in the position of demonstrating that they have done so – specific obligations to perform data minimisation assessments (either specifically, or as part of wide data protection impact assessments), and to properly document and make those assessments available, can be assigned to the relevant parties in the context of the Data Management Agreements which may be entered between them to regulate CAV data processing (as noted above). For example, collecting location data is invasive towards a data subject, since it can reveal essential and sensitive information[98] relating to them, such as information relating to their personal preferences, travel habits and relationships with others. On the one hand, manufacturers, developers and service providers could differentiate between data used for CAV training[99] and that used for the deployment of the CAV.[100] This could ensure that the personal data collected has a

whenever the resulting AI systems are socially beneficial and compliant with data protection rights." Furthermore, the use of data in training sets for algorithmic models should not be precluded when their inclusion is compliant with data protection rights and is socially beneficial. See European Parliamentary Research Service, *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*, June 2020, p. IV and p. 46. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf.

[92] European Data Protection Board, *Guidelines 05/2020 on consent under Regulation 2016/679*, Version 1.1, 4 May 2020, Section 3.2. Available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

[93] See European Data Protection Board, *Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications*, Section 1.5.3.

[94] European Parliamentary Research Service, *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*, Study of the Panel for the Future of Science and Technology, June 2020, p. 45. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf.

[95] See Article 5(1)(c) General Data Protection Regulation. Furthermore, note that this principle necessitates the processing of only the personal data which is strictly necessary for the purposes of the processing. For more information on the principle of data minimisation, please see the European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, 13 November 2019, p. 19. Available at: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en.

[96] European Union Agency for Cybersecurity, *Good Practices for Security of Smart Cars*, November 2019, p. 13.

[97] European Data Protection Board, *Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications*, Version 1.0, 28 January 2020, p. 14.

[98] "Sensitive data or data of a highly personal nature: this includes special categories of personal data as defined in Article 9 (for example information about individuals' political opinions), as well as personal data relating to criminal convictions or offences as defined in Article 10. An example would be a general hospital keeping patients' medical records or a private investigator keeping offenders' details. Beyond these provisions of the GDPR, some categories of data can be considered as increasing the possible risk to the rights and freedoms of individuals. These personal data are considered as sensitive (as this term is commonly understood) because they are linked to household and private activities (such as electronic communications whose confidentiality should be protected), or because they impact the exercise of a fundamental right (such as location data whose collection questions the freedom of movement) or because their violation clearly involves serious impacts in the data subject's daily life (such as financial data that might be used for payment fraud). In this regard, whether the data has already been made publicly available by the data subject or by third parties may be relevant. The fact that personal data is publicly available may be considered as a factor in the assessment if the data was expected to be further used for certain purposes", as explained in the Article 29 Working Party's *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, 4 April 2017, As last Revised and Adopted on 4 October 2017, pp. 9-10. Available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

[99] For example, training data sets could include synthetic data – meaning a simulated environment replicating the relevant features of the real world. Therefore, synthetic data allows for CAV manufacturers and service providers to simulate scenarios that are difficult to observe or replicate in real-life. This approach does not only serve for the safety of the CAV, but also for the utmost protection of data subjects' data subject rights and freedoms, as explained by the Organisation for Economic Co-operation and Development (OECD), *Artificial Intelligence in Society*, 11 June 2019, OECD Publishing: Paris, p. 98. Available at: https://doi.org/10.1787/eedfee77-en.

[100] European Commission, *White Paper on Artificial Intelligence – A European approach to excellence and trust*, February 2020, p. 19. Available at: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

specific and legitimate interest and minimising its use in other parts of the CAV's lifecycle. Additionally, limiting the use of the data in the deployment phase could help mitigate potential harms to data subjects. On other hand, according to recent research, the use of synthetic data can be used for the training of the CAVs' models, if it is available and affordable.[101] Synthetic input data would be able to train the AI system on complex situations and ensure for safer and more accurate CAVs.[102]

2.6 Transparency

Transparency[103] is closely related to the concept of fairness and the principle of accountability under the GDPR, where Article 5(2) GDPR[104] requires that the controller must always be able to demonstrate that personal data are processed in a transparent manner in relation to the data subject. Transparency is furthermore a fundamental enabler of user-centric processing[105] because it allows the data subject to understand and potentially challenge data processing that involves them. Without transparency and awareness of data processing activities data subjects cannot be in control of their data and exercise their rights. Being transparent involves the quality, accessibility and comprehensibility of the information provided. The information furthermore must be explainable. Transparency also acts as a promoter of trust in processes, which is required in order to ensure product uptake.

The principle of transparency is of particular relevance in the CAV environment insofar as the rationale behind automated decisions may significantly affect individuals and could even lead to life and death scenarios. In fact, ethical design is dependent on "the transparency of the technology and services in how that technology handles data, as well as providing choice for the user".[106] Individuals should be able to clearly understand the purposes and the limitations of data processing in the CAV,[107] as well as the expected level of accuracy with respect to the envisioned purpose and the conditions under which they can function as intended.[108] This is particularly complex in a situation where it "must always be possible to reduce the AI system's computations to a form comprehensible by humans"[109] and advanced technologies "should be equipped with a 'black box' which records data on every transaction carried out by the machine, including the logic that contributed to its decisions."[110]

A key element of transparency is found in Article 12 GDPR on Transparent information,[111] communication and modalities for the exercise of the rights of the data subject. Article 12(1), in fact requires that information relating to the processing should be provided to the "data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language".[112] This is no easy feat, however, as the actual audience may be different than the intended audience of the processing and adjustments may be necessary, especially over time, in situations where, e.g., the driver may not be the owner or regular user of the CAV. One way through which this may be mitigated is the use of standardized icons[113]

[101] Ibid.

[102] Organisation for Economic Co-operation and Development, *Artificial Intelligence in Society,* 11 June 2019, OECD Publishing, Paris, p. 98. Available at: https://doi.org/10.1787/eedfee77-en.

[103] See Article 29 Working Party, *Guidelines on transparency under Regulation 2016/679*, 29 November 2017, as last Revised and Adopted on 11 April 2018. Available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

Furthermore, note that the principle of transparency permeates throughout the diverse rules of the Maastricht DPCSR Framework. These specifically include the rules which fall under *Principle 1: Embed data protection and data security in the design of processes*, under which the rules of data security, ethics by design and user empowerment by design, and fairness by design are situated; and *Principle 2: Be transparent with citizens about the collection of their data,* which suggests using icons to signal that data processing activities are taking place. See Paolo Balboni and Kate Francis, "Data Protection as a Corporate Social Responsibility: From Compliance to Sustainability to Generate Both Social and Financial Value." European Centre on Privacy and Cybersecurity (ECPC), Maastricht University Faculty of Law website. 27 October 2020. Available at: https://www.maastrichtuniversity.nl/ecpc/csr-project/csr-publications.

[104] Recital 39 GDPR states, "… *that **(1)** any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. **(2)** Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be **(3)** adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum."*

[105] See Principle 1, Rule 2 Maastricht DPCSR, *Implement Ethics by design and User Empowerment by design, actively empowering individuals with respect to their data*, which calls for designers and producers of technologies and services to go beyond the requirements of user-centric design in order to actively empower individuals with respect to their data.

[106] Baldini et al. *Ethical Design in the Internet of Things*, p. 905. Sci Eng Ethics (2018) 24:905–925. https://link.springer.com/content/pdf/10.1007/s11948-016-9754-5.pdf.

[107] European Parliamentary Research Service, *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*, June 2020. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf.

[108] European Commission, *White Paper on Artificial Intelligence – A European approach to excellence and trust*, February 2020. Available at: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

[109] See Report with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)), A8-0005/2017, 27.1.2017, p. 10. Available at: http://www.europarl.europa.eu/doceo/document/A-8-2017-0005_EN.pdf.

[110] Ibid. Also see ICT Legal Consulting's contribution to nIoVe deliverable 2.1, section 4.3 on the Legal & Ethical Compliance of Defence Concepts. For more information about the project, see the nIoVe website. Available at: https://niove.eu/.

[111] Note that the Article 29 Working Party in its *Guidelines on Transparent information* to this end suggest making use of user panels to test the "intelligibility of the information and effectiveness of user interfaces/ notices/ policies etc." (See Article 29 Working Party, *Guidelines on transparency under Regulation 2016/679*, p. 8). Further to this requirement, the Article 29 Working Party notes the importance of the data subject being "able to determine in advance what the scope and consequences of the processing entails" which fundamentally means explaining the potential actual effects on the rights and freedoms of data subject, not limited to best case scenarios, but instead those which actually may severely affect individuals.

[112] The requirement of intelligible information "means that it should be understood by an average member of the intended audience" (see Article 29 Working Party, *Guidelines on transparency under Regulation 2016/679*, p. 7) and therefore requires the organization to "identify the intended audience and ascertain the average member's level of understanding." (see Article 29 Working Party, *Guidelines on transparency under Regulation 2016/679*, p. 8).

[113] The European Data Protection Board's Guidelines on CAVs suggest "informing the user that geolocation has been activated, in particular by using icons (e.g., an arrow that moves across the screen)", p. 13. Also see the CNIL's *Compliance Package on connected vehicles and personal data*, which "recommends that the data subjects be informed by: concise and easily-understandable clauses in the contract of sale of the vehicle and / or in the contract for the provision of services; and by using distinct documents (e.g., the vehicle's maintenance record book or manual) or the onboard computer; and using standardised icons in vehicles. The Commission strongly encourages the implementation of those icons to inform the data subjects in a clear, summarised, and easily-understandable manner of the processing of their data. In addition, the Commission emphasises the importance of standardising those icons, so that the user finds the same symbols regardless of the make or model of the vehicle." Available at: https://www.cnil.fr/sites/default/files/atoms/files/cnil_pack_vehicules_connectes_gb.pdf.

and sounds in CAVs pursuant to Maastricht DPCSR *Principle 2, Be transparent with citizens about the collection of their data, Rule 1: Before processing. The organization shall use icons (and sounds) for an easily visible, intelligible and clearly legible provision of information concerning the intended processing. Electronically presented icons should be machine-readable.*[114]

3 CONCLUSION: DATA PROTECTION AS A CORPORATE SOCIAL RESPONSIBILITY

As reflected in the above sections, the road towards compliance and ethical deployment requires CAV manufacturers, developers and service providers to come up with ingenious and novel solutions when designing and developing CAVs. Consideration of the GDPR-based obligations and the ePrivacy Directive requirements on consent and their application to CAVs unveils several unresolved issues, as seen in conflicts between restrictive legal principles, rules and requirements, on the one hand, and innovation on the other. As a result, organisations may struggle to fully meet their legal obligations. This paper has therefore sought to help address this problem by identifying several areas that are to be considered as potential priorities in designing and developing CAVs.

Concerning the GDPR predefined data processing roles, it is recommended to mirror the complex data processing relationships through multi-part Data Management Agreements which should aim to identify and regulate the variety of activities and relationships that exist between CAV stakeholders (see sub-section 2.1) . By properly configuring a Data Management Agreement, stakeholders can 1) map out the different types of CAV data processing activities which they are to perform, 2) identify the role or roles – independent controller, processor or joint controller – which apply to them in relation to each processing activity, and 3) set out the obligations to which each of them are bound as a result of the roles identified for each specific activity. This greatly reduces the risk of "grey areas" or undefined loopholes and ensures greater comprehensiveness and clarity of regulation of these complex processing relationships, for the benefit of CAV stakeholders and the data subjects concerned.

As a way to ensure data protection by design and by default, organizations should prioritise carrying out data protection impact assessments and IT security risk assessments prior to any processing activity and subsequently map the necessary technical and organizational security measures that would mitigate any high risks posed towards the rights and freedoms of data subjects (see sub-section 2.2). A *Data security by design* approach should entail adopting a by-design approach to security by integrating security best practices into the practices of the CAV stakeholder's organization on both the organizational and technical levels; human oversight and monitoring should also be ensured. CAVs should be designed in adherence to an *Ethics by design and User empowerment by design* approach which aims to actively oppose harm and empower users with respect to their data, ensuring that the positive societal benefits of CAVs can be reaped. More specifically, CAV stakeholders must consider *Fairness by Design* to regulate as well as prevent harm as a result of the algorithmic processing of the CAV, embedding fairness into the CAV itself (see sub-section 2.3).

Conflicts with the principle of purpose limitation may be balanced by applying compatibility tests when personal data needs to be used for other purposes, allowing for the reuse of personal data when the further purpose is compatible with the original purpose (see sub-section 2.4). Hand-in-hand with the principle of purpose limitation is the challenge posed to the principle of data minimization; whereby CAV manufacturers, developers and service providers are faced with the possibility of processing massive amounts of personal data and the obligation of only processing the personal data which is relevant and necessary for the envisioned processing activity (see sub-section 2.5). Other than carrying out the above test of what categories of personal data are relevant and necessary to process, CAV stakeholders could also differentiate between personal data used for the training stage and for the deployment and monitoring of the vehicle. Furthermore, transparency requirements are especially intensified in the CAV environment since the GDPR's expectations are that a data subject is able to understand the entire CAV processing (including the purposes, risks, recipients of personal data, etc.), as well as accurately comprehend the AI's computations and automated decision making. Creative solutions will be required on the side of the CAV manufacturers, developers and service providers in order to overcome this transparency obstacle, by way of standardized icons, sounds, and the possibility of changing the content and provision of information according to the audience at hand (e.g., drivers, passengers and children on board) (see sub-section 2.6).

While compliance with applicable data protection obligations represents an important starting point towards the lawful deployment of CAVs, reliance on existing legal privacy, data protection, and security frameworks is not enough to ensure a sustainable and beneficial proliferation of automated vehicles. In the case of new technologies and economic models that are constantly propelled into being thanks to perpetually-transforming innovations, regulation seems to come short in providing genuine protection of the fundamental rights and freedoms of Europeans and in effectively mitigating the risks presented by them. Due to the particularly high-risk nature of transportation and the extensive data processing operations that take place within the CAV in order to both make it function and make it enjoyable (infotainment) in fact, it is necessary that ethical concerns are adequately incorporated into the processes of developers, manufacturers, and service providers active in this environment.

The need for such an approach to data protection, one that can be considered as "ethical", which weds value-based models in the development of a newly virtuous form of compliance, going beyond what is prescribed by EU data protection law (ePrivacy directive and the GDPR) has already been confirmed by the European Data Protection Supervisor,[115] the European Commission,[116] and the

[114] Paolo Balboni and Kate Francis, "Data Protection as a Corporate Social Responsibility: From Compliance to Sustainability to Generate Both Social and Financial Value." European Centre on Privacy and Cybersecurity (ECPC), Maastricht University Faculty of Law website. 27 October 2020. Available at: https://www.maastrichtuniversity.nl/ecpc/csr-project/csr-publications.

[115] European Data Protection Supervisor, *Report Towards a digital ethics – EDPS Ethics Advisory Group.* 25 January 2018. Available at: https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf.

[116] European Commission, *European Group on Ethics in Science and New Technologies Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems.* March 2018. Available at: https://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf

Council of Europe,[117] among others. In the area of new technologies, such as CAVs, this regulatory gap can be met in the application of the principles that are outlined in the Maastricht University Data Protection as a Corporate Social Responsibility Framework. By following the Maastricht DPCSR Framework, operators in the automated vehicle sector can help ensure compliance not only with what is enshrined in the law, but also aim to provide added benefits for society, seeking not only to not cause harm, but to "do good" in the digital arena.

REFERENCES

[1] A Novel Adaptive Cybersecurity Framework for the Internet-of-Vehicles (nIoVe). H2020 Project. Grant agreement ID: 833742. Deliverable 2.1. https://niove.eu/

[2] Agencia Española de Protección de Datos, *Guía de Privacidad desde el Diseño*. October 2019. Available at: https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-desde-diseno.pdf

[3] Agencia Española de Protección de Datos, *Guía de Protección de Datos por Defecto*. October 2020. Available at: https://www.aepd.es/sites/default/files/2020-10/guia-proteccion-datos-por-defecto.pdf

[4] Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*. 4 April 2017. As last Revised and Adopted on 4 October 2017. Available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

[5] Article 29 Data Protection Working Party, *Guidelines on transparency under Regulation 2016/679*. 22 August 2018. Available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

[6] Article 29 Data Protection Working Party, *Opinion 03/2010 on the principle of accountability*. 13 July 2010. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf

[7] Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation*. 2 April 2013. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

[8] Article 29 Data Protection Working Party, *Opinion 08/2014 on the Recent Developments on the Internet of Things*. 16 September 2014. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

[9] Balboni, Paolo, "The Automated Vehicle Consortium and Fairness by Design." Blog post. May 2019. Available at: https://www.paolobalboni.eu/index.php/2019/05/08/the-automated-vehicle-safety-consortium-and-fairness-by-design/

[10] Balboni, Paolo and Kate Francis, "Data Protection as a Corporate Social Responsibility: From Compliance to Sustainability to Generate Both Social and Financial Value." European Centre on Privacy and Cybersecurity (ECPC), Maastricht University Faculty of Law website. 27 October 2020. Available at: https://www.maastrichtuniversity.nl/ecpc/csr-project/csr-publications

[11] Baldini, Gianmarco et al., "Ethical Design in the Internet of Things." *Science and engineering ethics* vol. 24, 3 (2018): 905-925. doi:10.1007/s11948-016-9754-5

[12] Charter of Fundamental Rights of the European Union. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:12012P/TXT

[13] Commission Nationale Informatique & Libertes, *Compliance Package: Connected vehicles and personal data*. October 2017. Available at: https://www.cnil.fr/sites/default/files/atoms/files/cnil_pack_vehicules_connectes_gb.pdf

[14] Council of Europe, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data adopted January 2017*. Strasbourg, France: Council of Europe, 2017. Available at: https://rm.coe.int/16806ebe7a

[15] Court of Justice of the European Union, C-582/14, Patrick Breyer v Bundesrepublik Deutschland, ECLI:EU:C:2016:779. Available at: http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1116945

[16] Court of Justice of the European Union, C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH, ECLI:EU:C:2018:388. Available at: http://curia.europa.eu/juris/document/document.jsf?text=&docid=202543&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1206721

[17] Court of Justice of the European Union, C-25/17, Tietosuojavaltuutettu v Jehovan todistajat, ECLI:EU:C:2018:551. Available at: http://curia.europa.eu/juris/document/document.jsf?docid=203822&doclang=EN

[18] Court of Justice of the European Union, C-40/17, Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV, ECLI:EU:C:2019:629. Available at: http://curia.europa.eu/juris/liste.jsf?num=C-40/17

[19] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national Supervisory Authorities responsible for the enforcement of consumer protection laws (Text with EEA relevance). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02009L0136-20091219

[20] Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment (Codified version) (Text with EEA relevance). Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32008L0063

[21] 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. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ:L:2016:194:TOC&uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG

[22] European Commission, *White Paper on Artificial Intelligence – A European approach to excellence and trust*. February 2020. Available at: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

[23] European Commission, *European Group on Ethics in Science and New Technologies Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems*. March 2018. Brussels, Belgium: European Commission. Available at: https://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf

[24] European Commission, Independent High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI*. 8 April 2019. Available at: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

[25] European Data Protection Board, *Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications*, Version 1.0, Adopted on 28 January 2020. Available at: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf

[26] European Data Protection Board, *Guidelines 05/2020 on consent under Regulation 2016/679*, Version 1.1., 4 May 2020. Available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

[27] European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*. 13 November 2019. Available at: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf

[28] European Data Protection Board, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, Version 1.0 , Adopted on 02 September 2020. Available at: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en

[29] European Data Protection Supervisor, *Connected Cars*, TechDispatch, Issue 3, 2019. Available at: https://edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-3-connected-cars_en

[30] European Data Protection Supervisor, *EDPS response to the Commission public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy*. 16 December 2015. Available at: https://edps.europa.eu/sites/edp/files/publication/15-12-16_online_platforms_en.pdf

[31] European Data Protection Supervisor, *Opinion 5/2018 – Preliminary Opinion on privacy by design*. 31 May 2018. Available at: https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf

[32] European Data Protection Supervisor, *Report Towards a digital ethics – EDPS Ethics Advisory Group*. January 25, 2018. Available at: https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf

[33] European Parliament. Charter of Fundamental Rights of the European Union. Luxembourg: Office for Official Publications of the European Communities. 26 October 2012. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:12012P/TXT

[34] European Parliament, *Report with recommendations to the Commission on Civil Law Rules on Robotics* (2015/2103(INL)), A8-0005/2017. 27 January 2017. Available at: http://www.europarl.europa.eu/doceo/document/A-8-2017-0005_EN.pdf

[35] European Parliamentary Research Service, Study of the Panel for the Future of Science and Technology, *The ethics of artificial intelligence: Issues and initiatives*. March 2020. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/634452/EPRS_STU(2020)634452_EN.pdf

[36] European Parliamentary Research Service, Study of the Panel for the Future of Science and Technology, *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*. June 2020. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf

[37] European Union Agency for Cybersecurity, *Good Practices for Security of Smart Cars*, November 2019. Available at: https://www.enisa.europa.eu/publications/smart-cars

[38] European Union Agency for Cybersecurity, *ENISA Programming Document 2020–2022 Including Multiannual planning, Work programme 2020 and Multiannual*

[117] Council of Europe, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data adopted January 2017*. 2017. Available at: https://rm.coe.int/16806ebe7a.

staff planning. Luxembourg: Publication Office of the European Union, 2020. Available at: https://www.enisa.europa.eu/publications/corporate-documents/enisa-programming-document-202020132022

[39] European Union Agency for Cybersecurity, *Towards a framework for policy development in cybersecurity, security and privacy considerations in autonomous agents*. March 2019. Available at: https://www.enisa.europa.eu/publications/considerations-in-autonomous-agents

[40] German Federal Ministry of Transport and Digital Infrastructure, *Ethics Commission Automated and Connected Driving*. June 2017. Available at: https://www.bmvi.de/SharedDocs/EN/publications/report-ethics-commission.pdf?__blob=publicationFile

[41] German Federal Ministry of Transport and Digital Infrastructure, *Task Force on Ethical Aspects of Connected and Automated Driving (Ethics Task Force) established by the 2nd High Level Structural Dialogue in Frankfurt/M. on 14 and 15 September 2017*. June 2018. Available at: https://www.bmvi.de/SharedDocs/EN/publications/report-ethics-task-force-automated-driving.pdf?__blob=publicationFile

[42] Government of The Netherlands, *Self-driving cars*. Available at: https://www.government.nl/topics/mobility-public-transport-and-road-safety/self-driving-vehicles

[43] Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659). *Ethics of Connected and Automated Vehicles: recommendations on road safety, privacy, fairness, explainability and responsibility*. 2020. Publication Office of the European Union: Luxembourg. Available at: https://ec.europa.eu/info/sites/info/files/research_and_innovation/ethics_of_connected_and_automated_vehicles_report.pdf

[44] Maastricht University. Developing a New Dimension of Data Protection as a Corporate Social Responsibility (DPCSR). Website. Available at: https://www.maastrichtuniversity.nl/ecpc/csr-project

[45] Organisation for Economic Co-operation and Development, *Artificial Intelligence in Society*, 11 June 2019. OECD Publishing: Paris. Available at: https://doi.org/10.1787/eedfee77-en

[46] 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. Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[47] United Kingdom Information Commissioner's Office, *Data protection by design and by default*. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/

[48] United Kingdom Information Commissioner's Office, *Principle (b): Purpose limitation*. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/

[49] United Kingdom Information Commissioner's Office, *Security*. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/

[50] WSP Canada Group Limited and Ontario Centres of Excellence, *Ontario CAV Ecosystem Analysis*. 2019. Available at: https://www.oce-ontario.org/docs/default-source/publications/avin-ecosystem-analysis-final-report-2019.pdf?sfvrsn=2