EXTENDED VEHICLE (EXVE) AND STANDARDISATION

PRESENTATION AND CHALLENGES OF THE EXTENDED VEHICLE

The “Extended Vehicle” is an international standard developed by the Automotive sector which encompasses the vehicle and its off-board servers. It is open to its ecosystem, but its interfaces are defined by the vehicle manufacturer, based on ISO standards. It provides a secure access to the vehicle’s data and was included in the provisions of the Strategic Contract signed between the automotive sector and the French Government on 22 May 2018.[1]

- It provides for a **coherent and interoperable management** of vehicle data;
- It protects the **safety of goods and persons and ensures the lawful processing of personal data** as it avoids watering down the responsibility of the controller and provides clarity regarding liability ;
- It provides for **equal treatment of stakeholders and ensures fair competition**.

The Extended Vehicle is currently being standardised at international level: several ISO norms defining the Extended Vehicle have either been adopted or are being finalised.[2]

RATIONALE OF THE OPPOSITION

Several categories of stakeholders oppose the Extended Vehicle, and specifically the standards on access to data for service development (ISO 20078 and 20080). This opposition focuses on two arguments:

1. The Extended Vehicle, as it is currently defined, **does not guaranty fair competition** between the vehicle manufacturer as service provider, and third-party services providers;
2. There is **an alternative** to the Extended Vehicle standard, which consists in an in-vehicle interoperable, open-access platform providing direct individual access to all service providers (“direct access”).

CHARACTERISTICS OF THE EXTENDED VEHICLE AND ANSWER TO THE OPPOSITION

Nevertheless, these two arguments do not hold when faced with a thorough analysis of the standards on the Extended Vehicle and the economics of B2B data sharing as provided in the “LOM” bill:

1. In order to prevent any infringement to competition rules, the ISO 20078 standard (web services) was subjected to a **competitive risk assessment** by the standardisation body which concluded that the standard did not carry any risk of anticompetitive behaviour. It provided for the possibility of appointing an independent, trusted third party which would be sole competent to grant data access right to stakeholders. Through this system, all stakeholders will be treated equally, including vehicle manufacturers, who will not be able to affect access rights.
2. **The Extended Vehicle provides and answer to several legal obligations:** security of goods and persons, IT security compliant with that used by the French Government for state digital services (France Connect), cybersecurity, fair competition, liability for products and data protection, as opposed to the proposed alternative.

The table below underlines the characteristics and advantages of the Extended Vehicle and the questions raised by the hypothesis of an unstandardised direct access to in-vehicle data, as no such standard currently exists.

[1] Contrat Stratégique de la Filière Automobile

[2] To date, several ISO standard defining the Extended Vehicle have either been adopted or are being finalised:

• ISO 20077 defines the general framework for the Extended Vehicle: ISO 20077-1 defines the concepts and terms for the Extended Vehicle; ISO 20077-2 specifies the methodology for designing the extended vehicle (security, safety).

• Two complementary standards provide for the use of the Extended Vehicle for over-the-air services: ISO 20078, currently awaiting the final vote of participants, provides the framework for the use of web services; ISO 20080, awaiting final vote, defines a first use case: Remote diagnostic support.

• Since early 2018, a new project for an ISO standard (ISO23132 « Road and ExVe Safety ») completes the set of standards regarding the Extended Vehicle. It covers the peri-vehicular communication of time constrained data relating road safety (e.g. V2V).

COMPARATIVE TABLE OF DATA ACCESS OPTIONS FOR CONNECTED VEHICLES

Evaluation Criteria	Characteristics of the Extended Vehicle	Questions relating to Unstandardised Direct Access
Technical Feasibility	• Ensured by an off-board server (over the air)	**Capacity**: an on-board solution would require as much equipment as in the vehicle it does stakeholders to ensure that there is enough storage. How can a single box, expected to respond to unidentifiable needs, could sustain the increased number of access requests? How could the issues relating to resources requirements be solved?
General interest/road safety	• Control over traffic safety and cybersecurity risks • Protection of users' interests (offense related sensitive data[3], speed, geolocation) • Equipment update (type-approval)	• **Cybersecurity**: Considering the number of stakeholders who will have a direct access to the vehicle's data, how can the risks created by the enlarged attack surface be contained? • **Sensitive data**: How can the distinction between personal data, sensitive data (offense related data) and non-personal data be ensured?
Economic Efficiency and Interoperability	• Best efficiency regarding the selection of data based on use-cases and aggregation requirements • Better coherence regarding data processing and related cost • Better chance of ensuring interoperability • Best method to facilitate French influence • Innovation integration	• **Economic balance:** How can it be ensured that multiple individual access does not negatively impact the economic balance of the system (costs) and competitiveness. • **Interoperability:** Direct access raises a crucial question regarding interoperability as it is not a solution common to all stakeholders. Rather it derives from multiple individual initiatives
Fair and Undistorted Competition	• Transparency: ISO standard published and discussed • Access condition applicable without distinction to all stakeholders, including manufacturers • *Ex ante* evaluation of the risks linked to anticompetitive behaviour • Authorisations managed by an independent organisation	• **Equal Treatment:** in a system with fragmented direct individual access, how can transparency, objectivity and non-discrimination can be ensured between stakeholders who do not have the same technical abilities and the same market power (e.g. new entrants)
Legal Certainty of the System	• Objective and transparent identification of the responsibility of the controller • Auditability of practices through data usage tracking	• **Data Protection:** Lack of identification of the controller (shared responsibility) • **Dilution/fragmentation of liability** due to a plurality of access

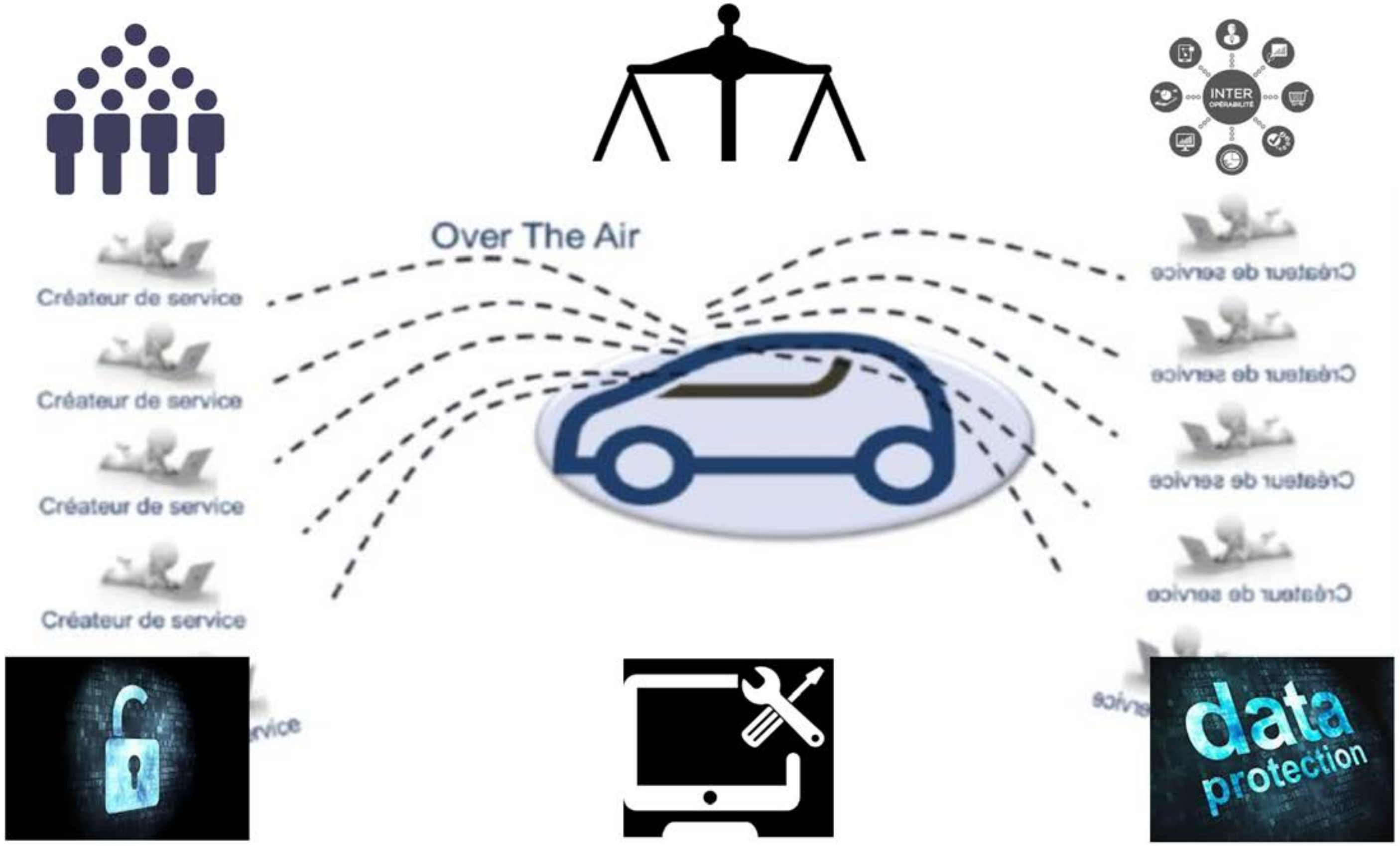
[3] Donnés sensibles d'infraction

QUESTIONS RELATING TO DIRECT ACCESS TO DATA

«Bufferisation » : CAPACITY ?

Differentiated Individual Access: FAIR COMPETITION?

Differentiated Access System: INTEROPERABILITY?



Access Dispersion: CYBERSECURITY?

Maintenance and Services Updates: TYPE APPROVAL?

Controller Responsibility: DATA PROTECTION?