FIGIEFA
Automotive Aftermarket Distributors

**FIGIEFA is working for you! #3**

**July 2021**

**A vast majority of the legislation for the automotive aftermarket is decided at European Union's or at United Nations' levels. They have a direct impact on your business. A single wrong, inaccurate or misplaced word could put the entire sector out of business. A strong political representation is needed to avoid that risk.**

**FIGIEFA represents independent automotive parts distributors towards European and international legislators. It monitors their legislative proposals and is in constant contact with them, with the aim to secure a legislative framework that allows you to operate your business and to thrive.**

FIGIEFA is working for you on

# Cybersecurity

at EU and UN levels

## *What is the issue?*

With the rise of connected and automated driving on one side, and the general increase of new cyberthreats on the other side, legislators worldwide felt the need to introduce regulation for addressing the issue of cybersecurity in the automotive sector. This is something which FIGIEFA is in favour of in order to protect motorists and unleash the potential of the market by ensuring confidence in new mobility technologies.

UNECE, a body of the United Nations dealing with mobility issues (among other topics), finalised in June 2020 two pieces of legislation on the matter, Regulation N°155 on 'Cybersecurity' and Regulation N°156 for 'Software Updates'. These Regulations will now be transposed into the European Union's legislation by mid-2021. These two Regulations on Cybersecurity and on Software Updates will become applicable, once adopted in the European Union, in 2022 for newly type-approved vehicles and as from 2024 for the existing vehicle park.

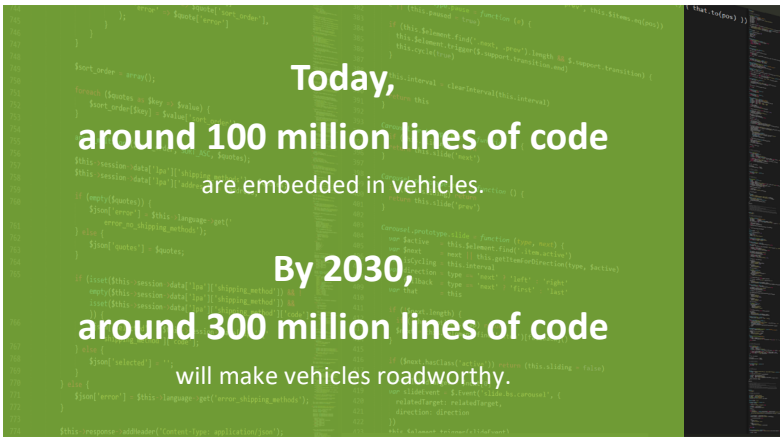
With Regulation n°155, UNECE has established an initial inventory of potential cyberthreats and corresponding mitigation measures. These mitigation measures however are not concrete implementation measures and give the freedom for vehicle manufacturers to implement their own proprietary security controls. They are now allowed to set their own benchmark (i.e. "what is adequate security?") and implement their own proprietary cybersecurity measures as part of vehicle type approval. Each vehicle manufacturer will create its own cybersecurity management system to set up organisational processes and implement security/software-update-related measures for each vehicle type. As a result, vehicle manufacturers can consider any access to and communication with the vehicle as a cyberthreat, and they can implement access control mechanisms and practices to address cybersecurity concerns (e.g. for the OBD port and wireless connection). The vehicle can be ring-fenced with vehicle manufacturers' proprietary cybersecurity measures and this has the potential to adversely affect the day to day operations of your companies.

## *How could it impact your business?*

As it stands today, this UNECE Regulation does not include any form of robust safeguard clauses for the automotive aftermarket. The proprietary cybersecurity strategy of the vehicle manufacturers could make it impossible to use spare parts from independent sources, as they could be rejected by the vehicle in the name of 'security'. This exclusion could have a profound and negative impact on your entire portfolio of spare parts identified as "cybersecurity relevant" (e.g. any part with electronic components), especially those which are not sourced from original equipment suppliers .

Impediments to free competition in the automotive aftermarket could be extended even further under the argument (or even pretext) of 'cybersecurity'. First examples are access restrictions to the OBD port via proprietary vehicle manufacturers' security certificates, proprietary vehicle manufacturers' codes (QR codes or software) needed for the activation of spare parts (often with vehicle manufacturers' own diagnostic tools) or the general prevention of remote communication with the vehicle and its data. All these restrictions could now be imposed widely under the legal requirements of cybersecurity protection.

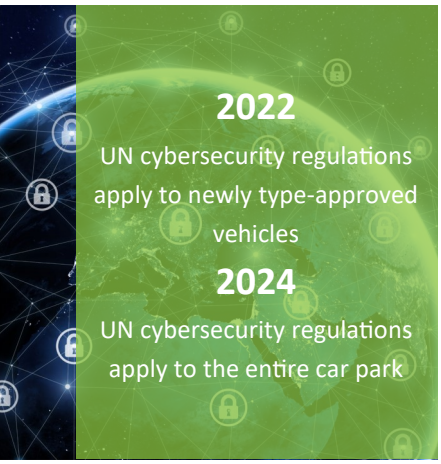
This would prevent independent, multi-brand businesses to conduct a wide range of repair and maintenance services and drive further consumers into the vehicle manufacturers' contracted networks.



## *What is FIGIEFA doing?*

FIGIEFA fully supports measures to protect connected vehicles against cybersecurity threats. However, the process of cross-referencing of the UNECE Cybersecurity Regulations into the European Union's legislation should not lead to granting vehicle manufacturers a total arbitrary control of the cybersecurity implementation. The European Union must take the necessary measures to avoid that the entire automotive aftermarket (and related digital and mobility value chains) is disrupted.

This is why FIGIEFA, together with other aftermarket, leasing/rental companies and consumer organisations organised in 'AFCAR' (Alliance for the Freedom of Car Repairs), is currently in the process of informing European Union's officials and Member States representatives to raise awareness and gather support. The objective is to ensure that the transposition of the UNECE Regulations into the European Union's legal framework is accompanied by robust implementation clauses to ensure that all stakeholders continue to have the ability to operate, in a non-discriminatory and competitive manner, whilst addressing cybersecurity. Without such measures, the aftermarket would be at risk.




In more details, FIGIEFA is calling upon decision-makers to ensure i.a.:

- cybersecurity compatibility and interoperability for replacement parts;
- cybersecurity compatibility and interoperability for multi-brand diagnostic tools;
- setting-up a European Union-wide certification scheme, by extending the current SERMI scheme to cybersecurity (including also an approval and authorisation scheme for diagnostic tools and any other operator involved in providing mobility services;
- amending the provisions on the OBD port to define rules for the period of proprietary issuing of security certificates by vehicle manufacturers until the European Union-wide certification scheme is set-up.

In parallel, FIGIEFA is organising technical meetings with spare parts experts to work on concrete implementation requirements for cybersecurity, and is arranging informational webinars to prepare FIGIEFA members for cybersecurity.

Last but not least, FIGIEFA commissioned an independent cybersecurity study, with the aim to show that it is perfectly possible to have the highest level of cybersecurity protection, whilst at the same time allowing an independent communication with the vehicle, its data and resources.


**The outcome of the political discussions on this issue will have a decisive impact on our sector. FIGIEFA will keep defending your interests in the upcoming months to make sure that your companies don't get hampered from conducting business. We will need your support to strengthen our activities and to convince political decision-makers of the importance of taking into consideration your needs. Stay tuned!**

Any question on the topic? **Contact our expert, Hari Ramakrishnan (hari.ramakrishnan@figiefa.eu)**

Boulevard de la Woluwe 42
1200 Brussels
Belgium

figiefa.secretariat@figiefa.eu
+32 2 761 95 10

www.figiefa.eu
@FIGIEFA
/figiefaeu

/FIGIEFA
/figiefa