
The Cybersecurity of Autonomous Vehicles and Public Regulation: Why Should Policy Makers strive for a Standard-Based Regulation instead of a Rule-Based Regulation ?

Bashar Fteiha*¹

¹Bashar Fteiha – Pays-Bas

Résumé

The automotive industry is undergoing a huge transformation with the introduction of Autonomous Vehicles (AVs), which are likely to revolutionize our transportation systems. While the benefits of AVs are widely discussed, a major issue at the heart of this discussion is that of cybersecurity and whether they are secure against cyberattacks. In this respect, policymakers are faced with the demanding challenge of formulating an effective legal framework to regulate cybersecurity with regards to AVs. However, one of the primary concerns for the policymakers is what type of regulation should be implemented- should it take the form of rules-based regulation or standards-based regulation? A rule-based regulation consists of explicit, clear, and detailed rules regarding permissible and impermissible conduct in relation to the cybersecurity in AVs. In contrast, a standard-based regulation offers a more flexible approach, as it provides considerations and options that allow the relevant actors to use their individual judgment and discretion when determining which cybersecurity measures to implement with regards to AVs. While the debate on how to regulate the cybersecurity of AVs has intensified in Europe, there has been little focus on the structure of this regulation and the extent of precision needed.

This contribution asserts that a standard-based regulation is the most efficient and suitable legal approach to regulate the cybersecurity of AVs. This can be better understood when one takes into account the pacing problem of technological innovation and the limited ability of the law to keep up. Rapid advancements in technology, such as those pertaining to AVs, generally occur at a faster rate than the law, making legal rules outdated. Consequently, a rule-based regulation which precisely outlines the security measures that must be taken by relevant actors runs the risk of becoming obsolete due to its rigidity. Additionally, the costs involved in the promulgation, interpretation, and application of a rule-based regulation are relatively high. On the other hand, a standard-based regulation allows for more flexibility and offers the ability to keep up with the changing security needs of the AV industry. As such, if a certain security measure were to become irrelevant over time, a standard-based regulation would be able to capture this evolution more easily compared to a rule-based regulation, which would need to be reformed.

Besides, the manufacturers of AVs and third parties involved in the development of these vehicles are well-versed in the best cybersecurity practices and measures, and they are more

*Intervenant

capable of keeping track of the latest developments on cybersecurity. Therefore, a standard-based regulation gives these actors the freedom to determine which measures will be most effective in light of recent developments. On the contrary, a rule-based regulation which sets out detailed cybersecurity requirements may not yield the best results, as relevant actors could be encouraged to only implement up to the pre-defined measures, even if more effective security measures become available in the future. Hence, the evolving nature of cybersecurity and its elements that affect the levels of security make a strong argument in favor of a standard-based regulation.

Mots-Clés: Public Regulation, Rule, based Regulation Standard, Standard, based Regulation, Law and Economics, the Cybersecurity of Autonomous Vehicles and Incentives structures