Maria Ostashenko Partner
mostashenko@alrud.com

Anastasia Petrova Associate
apetrova@alrud.com

Dmitry Simbirtsev Junior Associate

ALRUD Law Firm, Moscow

Image: Yulia Vambold / Unsplash.com

Russia: Automotive Strategy envisages legislative changes for autonomous vehicles

Autonomous vehicles are no longer a concept of the future and with their introduction comes the need to address data privacy and cyber security concerns. Maria Ostashenko, Anastasia Petrova and Dmitry Simbirtsev, Partner, Associate and Junior Associate respectively at ALRUD Law Firm, discuss how the Strategy for the Development of the Russian Automotive Industry ('the Strategy') seeks to address these issues.

The Automotive Strategy in context

The principal Russian producer of city transportation vehicles has recently announced that the first autonomous tram in Russia will be tested in Moscow in autumn 2018.

Technology is currently advancing faster than the law, as Russian legislation does not yet provide comprehensive guidance on how basic traffic rules shall apply and how to address numerous regulatory, data privacy and cybersecurity concerns surrounding technology, such as autonomous vehicles.

In order to address the above concerns and instigate inevitable legal changes, Russian law and policymakers have given a special and detailed consideration to autonomous vehicles in the Strategy, adopted on 28 April 2018. The Automotive Strategy is designed to summarise the current state of affairs in the Russian Automotive Industry and how it will change in the future.

Data ownership

Automated systems within autonomous vehicles collect a huge volume of information, which is processed in real time to ensure the proper operation of the vehicle. The primary concern in this regard is how this type of information shall be governed and, accordingly, which specific obligations will be imposed on the entities involved in the operation and use of such vehicles. It appears that this question may not remain unresolved, since the answer to be given predetermines how this information may be circulated.

In particular, the Automotive Strategy defines data security in relation to the operation of autonomous vehicles as the key issue to consider in the near future.

Privacy issues

Personal data is defined in Russian legislation as any information related to a directly or indirectly identified or identifiable individual. In reality, the notion of personal data is construed rather broadly, so in certain cases the line between technical information and personal data appears unclear. Although the Internet of Things and Big Data are mentioned among other key areas of information society within the Automotive Strategy of Information Society Development in Russia, adopted by the President on 9 May 2017, they still remain in a grey area

giving rise to certain privacy concerns.

This issue is of practical importance. If data collected by autonomous vehicles is considered personal data, a number of obligations shall apply to processing of such data, such as defining a responsible data controller, ensuring legal grounds to data processing, including rapid and unpredictable data transfers between data controllers and data processors, as well as the localisation of databases.

The Automotive Strategy specifies the necessity of amending Russian legislation on personal data in order to address issues related to processing and transfer of personal data by autonomous vehicles.

Cybersecurity issues

Autonomous vehicles are not ordinary vehicles; they are well developed automated systems connected to hubs, communicating with each other through information transfer. Information security systems designed for the operation of autonomous vehicles have the same priority as the quality of auto parts used. Unauthorised access to the vehicle's systems may cause malfunction and in turn a collision on the road.

In addition, cyber terrorism is a significant global problem, so it must not be ignored that autonomous vehicles are already a target. Therefore, the information security of each individual vehicle is a matter of public security as well. It is for the regulator to ensure that autonomous vehicles admitted to public roads are properly secured from cyber-attacks. This will likely be achieved through the elaboration on current, and the implementation of new technical standards, met by vehicle manufacturers, especially when they want to sell their products to the local market.

In addition, the period of a vehicle's use is usually longer than that of a smartphone. From a practical perspective this means that manufacturers cannot simply stop providing technical support to their vehicles once a new model is introduced to the market. Given the greater security concerns with regard to autonomous vehicles, mandatory minimum service periods and rules for its calculation, will be defined.

Critical infrastructure law

The future use of autonomous vehicles prompts the development of the respective infrastructure. The Automotive Strategy acknowledges this and provides for the following measures in this direction: the creation of a special area for the autonomous vehicles trials, designing special transport corridors for autonomous vehicles and the development of special technical facilities to ensure proper operation of the whole transport system where autonomous vehicles are driven alongside traditional vehicles.

In other words, making this dream a reality requires the creation of special infrastructure, which shall be properly protected from cyberattacks and intrusions both technically and legally.

On 1 January 2018, Federal Law of 26 July 2017 No. 187-FZ on the Security of the Critical Information Infrastructure of the Russian Federation ('the Critical Infrastructure Law') came into force. The Critical Infrastructure Law targets state authorities, Russian legal entities and individual entrepreneurs owning and otherwise possessing IT and telecom systems, automated control systems, as well as electronic communications networks applied in industries including healthcare, science, transport, communications and defense. It also applies to the Russian entities and individual entrepreneurs ensuring connectivity between them.

The forthcoming daily use of autonomous vehicles implies the development of new infrastructure and given their security has a great importance, newly introduced regulations on critical infrastructure are also necessary. In contrast, the question of autonomous vehicles' prospective applicability to such infrastructure shall be necessarily raised, since the mere answer thereto will be meaningful to determine who can own systems comprising the infrastructure, and what responsibilities such an entity will bear (the ones set out by the regulations on critical infrastructure are rather comprehensive and strict).

Telecom issues

Autonomous vehicles are driven and exchange information with use of the internet. It is already possible to track unmanned vehicles with use of GPS signals. The Automotive Strategy emphasises the necessity of developing new technologies of wireless data transfer, that will allow autonomous vehicles to exchange information immediately. Currently, Russian legislation does not provide standards for requisite telecom systems and there are certain difficulties in implementation of such telecom systems due to the unresolved question of electromagnetic capability.

Public security issues

Russian national defence legislation provides for a number of restrictions aimed at the provision of national security and military defence amongst other things, such as the prohibition of obtaining information comprising state secret, prohibition of use of a software for surreptitious obtaining of information, and restricting entrance to the zones where military and other objects crucial for national defence are situated.

Due to these restrictions, it seems that two options are possible. The first, implies that the use of autonomous vehicles in such areas should be prohibited. Meanwhile, under the second option, which is more complicated, the regulator will introduce (or adapt current ones, such as licensing) specific requirements to the vehicles designed to be used in such areas, and also to their manufactures.

Notwithstanding the above scenarios, it leaves no room for doubt that the state security legal restrictions will have an impact on the industry and its further development.

Conclusion

The Automotive Strategy is clear about the intentions to introduce autonomous vehicles to public roads. Hopefully, the Automotive Strategy will not be considered a mere declaration, but a call to action. It will be time and energy consuming, as it requires big reforms on multiple fronts. It also seems to be very challenging for the regulators, who will have to find a balance and consistency with the regulatory approaches to the information security of autonomous vehicles and transport infrastructure, along with the adaptation of the current traffic rules for their use.