Killer cars? Autonomous vehicles and criminal liability

Dalit Ken-Dror Feldman

*Who is criminally responsible when an autonomous car is involved in a car accident such as the accident in Arizona? The immediate suspects include: the user, the software company, the car manufacturer, the car itself and a hacker. In this blogpost **Dalit Ken-Dror Feldman** takes a closer look at this questions and answers it from the perspective of the basic principles of criminal law.*

Autonomous vehicles differ in degrees of automation. The Society of Automotive Engineers International suggested 6 levels of driving automation in 2014. When we talk about autonomous vehicles we refer to level 3 and above, where the automated driving system monitors the driving environment.

During the training process, as well as afterwards for private use, autonomous vehicles might be involved in car accidents, as indeed happened already in Florida in 2016, when the passenger of the car was killed. During 2018 we witnessed a new autonomous vehicle accident. This time the victim was a pedestrian who crossed the road in Arizona. It is time to decide who is to be held liable as the offender.

Who is to be prosecuted?

The list of potential offenders regarding autonomous car accidents includes:

- The user
- The software company
- The car manufacturer
- The robot – the car itself

- A hacker

In order to decide whom society should find as the criminal offender, we need to keep in mind the basic justifications of criminal law, among them: Proportionate punishment, general deterrence (prevention),rehabilitation, and education (individual deterrence).

Prof. Gabriel Hallevy, in his article “I, Robot – I, Criminal” talked about 3 models that could be applied to AI: (1) direct liability – prosecute the car (“the Direct liability model”); (2) offence by proxy – prosecute the user, the car manufacturer or the software company who caused the car to commit an offence (“the Perpetration-by-Another liability model”); (3) the natural and reasonable consequences – prosecute the person who should have foreseen the result of his actions or inaction (“the Natural-Probable-Consequence liability model”).

Should we prosecute the car?

In my opinion, if we check the basic principles of criminal law, in the meantime, the first suggested model is not relevant. If cars cannot feel or be afraid of punishment almost no rationale of the criminal system can justify its punishment. A slight justification of this model might be that the car can be shut down and be given a “death punishment,” while the problem in other cars should be fixed. That can be explained maybe under the basic principle of proportionate punishment.

Can we prosecute a hacker (cracker)?

If there is proof that the system was hacked, then the state should prosecute the hacker. The software designer might be also considered as an offender if he did not use the state-of-the-art security system to protect the car from being hacked, according to the natural and probable consequences model.

So, who should be considered as an offender?

Full automation – stage 5: In stage 5 of autonomous cars the passenger will not be able to control the car and hence the basic principles of criminal law are not met.

If the passenger is not the driver and cannot decide whether to act in a certain way or not, there should be no criminal liability on him. Punishing him will not teach any other driver to act in a different way, there is no process of rehabilitation for the passenger and if he does nothing wrong (because he is not in control of the car) to punish him is not proportionate.

Moreover, if we try to prosecute a passenger that may be a child, a drunk or any person that does not possess a driving license or cannot drive – we will pull the rug underneath the whole idea behind the autonomous car.

To prosecute the car manufacturer or the software company is more logical according to the basic principles of the criminal law – i.e. – if there is a problem with the car itself. The principles of general deterrence (prevention) and education (individual deterrence) of the two and of others in the field are also relevant . Both of them can still prove that they acted without criminal intent and without negligence and did everything possible to prevent the offense.

The car owner can be found as the offender just if he changes the software or hardware to an unverified version or does not install the relevant patches as long as it falls into the natural and probable consequences model. If the driver changes the car – and because of this unverified version of software or hardware an offense is committed, in order to deter other drivers from doing the same the driver can be and should be convicted. In addition the driver should be proportionality punished for his acts.

Semi automation – stages 3-4: We should keep in mind that until stage 5 has been reached, there should be an alert driver in the car and the advantages of the autonomous vehicles will be reduced. In stages 3 or 4, where the passenger is still considered as a driver (with a valid driving licence) who should handle difficult situations, the driver will be liable as an offender according to the current criminal system. As long as the driver is responsible for driving the car and for his acts in the car or lack of them – the basic principles of the criminal law are still met.

The driver can still prove that he acted without criminal intent and without negligence and did everything possible to prevent the offense, or that he did not have enough time to act or that the car was hacked. In addition, if the driver decides to act when there is no car warning, then he should be convicted (or not) according to the current criminal law. Alongside, the car manufacturer or the software company can be prosecuted as well if their acts or lack of them caused the offence.

In all stages – using the same logic, if the system is hacked (and the offence occurs due to that) we should prosecute the hacker (cracker) and we should prosecute the software company if it did not provide sufficient security.

Summary

Before deciding on the attribution of criminal liability in the field of autonomous vehicles, we should bear in mind the different basic principles of criminal law. As was explained previously – in stage 5 there is no rational to prosecute the car owner and the passenger as long as they install all the relevant patches and do not change the software or the hardware. The car manufacture or software company will still be able to prove they acted without criminal intent and without negligence and did everything possible to prevent the offense.

In stage 3-4 – the current criminal system is relevant assuming that there is a duty for an alert driver to be on board.

In all stages – if the system is hacked we can prosecute the hacker (cracker) and the software company in the relevant cases.

In addition, we can also think about creating systems of heavy fines and punishments if a malicious conduct is involved. However, we will leave this for further considerations.

As for the robot, the car can be shut down – however as long as the car (and all the other cars) cannot feel or be afraid – the basic rationales of the criminal system are not met. Stage 5 autonomous vehicles are just around the corner. It is time to decide. A clear attribution of criminal responsibility should be made – the sooner the better.