



Strasbourg, 10 March 2019

CDPC(2019)8

EUROPEAN COMMITTEE ON CRIME PROBLEMS (CDPC)

DRAFT QUESTIONNAIRE CONCERNING ARTIFICIAL INTELLIGENCE AND CRIMINAL JUSTICE

Document prepared by the CDPC Secretariat
Directorate General I – Human Rights and Rule of Law

1. Does your national legislation address liability issues connected to automated driving or any other form of robot -human interaction (such as medical surgery or industrial work)?

If so, could you please:

a) provide, if available, the relevant texts (in English or in French);

b) indicate whether responsibility is allocated to a specific person (e.g. *driver, producer, programmer, etc.*) and on what standard it is based (*i.e. strict liability, negligence, intention?*)

2. Please choose the answer that seems most appropriate for your jurisdiction:

If a (legally authorised) self-driving car runs over a child, prosecution is not possible, because a robot:

a) has no standing under the law, i.e. no personhood;

b) cannot meaningfully act (as a criminal law subject);

c) cannot be found guilty, i.e. is not able to receive a criminal punishment due to lack of moral agency.

3. Are lawmakers (or academic scholars) discussing the possibility of granting personhood to a robot (a so-called e-person) in your State?

4. According to your law does negligence require:

a) foreseeability and/or;

b) preventability;

c) strict liability?

(please note, requirements could be problematic when robots are “self-teaching” so that their actions can neither be fully predicted nor prevented (by producer, programmer, user).

5. Does your national legislation address the problem of “complicity in negligence”, i.e. various actors collaborate possibly each violating “due care” and cause harm to third persons; but in retrospective it is impossible to proof who caused the harm (for instance in the case of an automated driving car killing a pedestrian, when it is impossible to prove whether one of the programmers coded faultily or the map data provided was erroneous).
6. Does your criminal justice system reflect the idea of a “socially permissible risk” a risk that even if it materialises, will not lead to prosecution in the light of the overall social benefits associated with the risk-taking?
(Such a notion is prevalent in modern life in general, and motorised traffic in particular. It is legal to drive a car even though this can lead to a lethal incident without anyone being at fault.)

7. Does your law require compliance with state of the art technology (e.g. safety and security of a robot) with the consequence that criminal liability can be imposed in the case of non-compliance, but no criminal liability in the case of compliance?

Is there a general rule of liability for companies (similar to Art. 12 of *Convention on Cybercrime*, ETS No.185 and many other CoE criminal law conventions obliging States to ensure corporate liability)?

8. Does your domestic legislation have
 - a) a definition and/or;
 - b) specific regulation for the obtainment, presentation and evaluation of digital evidence, i.e. evidence that is stored electronically?
9. Are there problems with digital evidence in practice?
If so, please explain briefly.
10. Are there problems when data is located in another country?
If so, please explain briefly.
11. Do you often (quantify xxx) face the situation where data is stored with a Cloud Service Provider?
If so, please explain briefly.
12. Do you think the Council of Europe Convention on Cybercrime ETS No.185 is effective in addressing cybercrime issues and dealing with cross border access to evidence? If not, please specify.
13. Do authorities in your jurisdiction use digital analytical tools to produce forensic results (i.e. DNA analysis kits or breathalysers)?
If so: Are there specific safeguards in place to ensure reliability of such evidence, e.g. disclosure of underlying data like the source code, machine learning parameters, etc.?
14. Do authorities in your jurisdiction use profiling tools (i.e. risk assessment in the judicial system or in prisons and predictive policing)?