Strasbourg, 7 November 2019 CDPC(2019)17

EUROPEAN COMMITTEE ON CRIME PROBLEMS

(CDPC)

ASSESSMENT OF THE ANSWERS TO THE QUESTIONNAIRE ON ARTIFICIAL INTELLIGENCE AND CRIMINAL JUSTICE (using the example of Automated Driving)

Document prepared by Dr. Sabine Gless & the Working Group

in co-operation with the CDPC Secretariat
Directorate General I – Human Rights and Rule of Law

www.coe.int/cdpc | dgi-cdpc@coe.int

Table of Contents

Contents

A. Introduction

1. The increase in new technology driven by **Artificial Intelligence (AI)** presents legal challenges for each member State as well as for the Council of Europe (CoE), as a pan-European organisation (https://www.coe.int/en/web/artificial-intelligence/home). The Council of Europe Committee on Criminal Problems (CDPC) is addressing these important issues in a project using driving automation (coe.int/cdpc-2018-14rev-artificial-intelligence-and-criminal-law-project-2018-/16808e64ad) as a widely diversified everyday example of (narrow) AI. This bundling together of IT techniques enables human co-operation with driving systems, i.e. robots that interact with each other as well as with a human user in order to (temporarily) take over the driver's tasks. The industry distinguishes between different levels of **driving automation** (Norm SAE J3016_201401). Of current interest are the transitions from level 2 onward to levels 3 and 4. At level 2, a car can execute dynamic driving tasks, but the driver must monitor and overrule the system, if necessary. At level 3, a driver no longer needs to monitor the system when activated, but must respond to a takeover request. **Level 4 automation** is used for various 'mixes' of highly automated and fully automated driving depending on the focus; it especially covers situations in which the driver does not respond to a take over-request (TOR) and the car is expected 'minimize' the risk resulting from this situation. Level 5 envisages autonomous driving without a human driver. The manifold forms of **driving assistants** draw on miscellaneous forms of machine learning-concepts for varied functions (e.g. lane and distance keeping, parking, infotainment, drowsiness detection). Driving assistants used for safety relevant features are normally "frozen" before the system is integrated in a car model, i.e. their learning process will not continue on public roads (see www.unece.org/fileadmin/DAM/trans/doc/2018/wp29/WP29-175-21e.pdf). However, in order to be able to function on the road, driving assistants must be adaptive, i.e. capable for a specific operation based on autonomous data obtainment and evaluation. Thus, driving assistants embody AI risks (autonomy, connectivity and human-robot-interface) on different scales.

2. This report follows up on the thematic session on AI and criminal law responsibility held in November 2018, when CDPC set up a working group of experts representing member States supported by scientific experts (hereafter the Working Group). The Working Group prepared a questionnaire (Annex 1) that was sent to all CoE member States in order to both analyse the

national measures taken in the area of AI and criminal law and to identify whether there is a need for CDPC action. 36 member States had replied by 12 November: Andorra, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Italy, Moldova, Monaco, Montenegro, North Macedonia, Norway, Latvia, Lithuania, Luxembourg, Poland, Portugal, Romania, Russia Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and Ukraine. This report gives a broad overview based on the answers provided by member States as well as on discussions in the Working Group. Data protection and cyber security are not part of our focus since those subjects are followed by other relevant CoE bodies.

B. Preliminary findings based on an analysis of the replies from member States regarding self-driving vehicles

I. CoE instrument on AI and criminal justice

The legal problems caused by the employment of AI in everyday life, as with driving automation, is of huge interest to CoE member States and many CoE bodies. The high response rate to the questionnaire and the many detailed explanations illustrate this, as well as the positive assessment of the CDPC project by the Parliamentary Assembly's Committee on Legal Affairs and Human Rights (Memorandum adopted on 26 September 2019 AS/Jur (2019) 36 on "Legal aspects of 'autonomous' vehicles"). It is clear that the advent of the digital era, in particular the development of the automotive sector, affects many citizens as well as the industry making such technology available on the European continent. This is a compelling reason to explore new options in addressing the issues raised by AI for criminal justice. The Working Group considered and agreed that a CoE instrument should be prepared without indicating a specific form.

II. New domestic regulation for driving automation

1. Up to now only a few member States have prepared or already adopted **general legislation** which may affect **criminal liability** when humans hand over the steering wheel to driving assistants, in particular with regard to requirements for negligence. A larger number of States have adopted regulations for driving automation **pilot projects**. Also, one country has adopted

regulations for pilot projects, and is considering adopting general legislation regarding liability issues in driving automation (France). Many replies disclose that while most member States have not yet adopted new legislation for driving automation, there is a necessity to do so, at the latest when “self-driving cars” can go on public roads without a human driver inside.

2. An analysis of new rules, where already adopted or under consideration/preparation shows that up to now, only a few countries have adopted **general provisions** for using driving automation or plan to do so (Austria, Germany, France and Switzerland), while other member States have adopted specific regulations for **pilot tests**.

3. At the current time, even when adopting new regulations, member States typically remain rooted in traditional notions with regard to liability schemes. In particular, no country has yet opted for the creation of a new legal notion (such as an “e-personhood”) which takes into account that based on AI a vehicle could in fact engage in dangerous driving itself, not as a consequence of human action. At the same time, legal provisions aim to assign responsibilities in this new situation of human-robot interaction. In principle, two options are available: (1) All responsibility remains with the human driver, such as in Austria where Art. 3 (2) of the Austrian Regulation (*AutomatFahrV*) explicitly states: “The driver may transfer certain driving tasks to [authorised driving assistance] systems, but remains responsible at all times for resuming all driving tasks.” or (2) Drivers may divert from the traffic situation and hand over the vehicle to driving assistants as long as they use automatic driving functions properly and are ready to respond to a takeover request at any time, §§ 1a and 1b German Road Traffic Act (Strassenverkehrsgesetz).

4. If the human driver is not legally required to monitor traffic until a takeover request is issued by the driving assistant, he or she, in principle, cannot be held responsible for the driving activity during this time. As a consequence, when the automated system is activated **drivers should not be held criminally liable, in principle, if an incident occurs in automated mode** and the human driver complies with all rules, as they are legally discharged from driving obligations when using a driving assistant compliant with authorisation. However, a driver will have to take over the control of the vehicle when there is a takeover request. If a driver does not take over or causes an accident, he or she will be held responsible. This set-up creates a demanding situation for the human driver who faces actual tasks of reacting quickly and at the right time, and must comply with many more new obligations (partly to be found in the car’s user manual).

The reluctance to acknowledge AI driven systems as actors that take decisions and can cause harm might challenge criminal justice systems in the long run with no answer to the frequently asked question: Who is responsible if an automated driving car runs over a human?

5. Member States, which have chosen to regulate test driving only, often decide on a **case by case basis**. It is rather difficult on that basis to draw a general conclusion about a common direction for such regulation. Generally speaking, however, in such schemes, the drivers (as well as permit holders for such pilot tests) may remain liable. The Italian "smart road" decree of 28 February 2018, for instance, allows for test driving of self-driving cars, but expressly recalls Art. 196 of the Highway Code and Art. 2054, paragraph 3, of the Italian Civil Code, which implies a solidary (administrative and civil) liability for both the owner and the driver.

6. All member States acknowledge the **necessity of data monitoring and storage** without, however, addressing particular criminal justice concerns (like privileges against self-incrimination or protected privacy spheres). The relevant Austrian and German laws, for instance, require that all data generated during automated driving must be registered and, on request, transmitted to the authorities responsible for monitoring road traffic, which could have manifold consequences for criminal investigations.

III. Liability issues

1. Member States without specific legislation for the use of driving automation apply **traditional, i.e. 'general' liability rules** at this point in time, despite having changed the traffic laws to make them suitable for the use of highly-automated or autonomous (test) driving. They recognize the risk **of a distorted assignment of responsibility** or **even responsibility gaps** and the necessity of legal changes when driving assistants replace drivers. Some countries point out, for instance, that when "autopilots" (which are functioning in a car, although they are not certified as "self-driving systems") replace drivers, the consequence of human drivers' liability for any "act of that system" may seem unfair. Furthermore, where governments embrace legal reforms in traffic law (for instance, with regard to the Vienna Convention on Road Traffic made in the UNECE Global Forum on Road Safety), a follow up in other areas of law seems necessary. In a nutshell, it appears that member States agree on the **compelling necessity for new regulation, at the latest when "cars drive by themselves",** yet some lack a convincing approach as these

issues pertain to crucial elements of their criminal law, like culpability or legally-relevant action based on an autonomous will or personhood of non-human actors.

2. Facing the emerging responsibility gap when driving assistants take over the steering wheel, the member States start with different sets of traditional rules, which will not be explored here in detail. It is, however, important to note that the characteristics of existing liability models do, to a large degree, account for a different focus when looking ahead.

3. The human **driver**, for instance, is a central figure for criminal liability in all member States. However, the member States' legal approaches to defining who is actually considered a driver differ widely. While some focus on "**those who sit behind the wheel**" others apply a more open approach, and include **"remote drivers"** or **"operators"** or possibly an **"officer for the monitoring of the operation of a vehicle"**. With test projects in driving automation still underway, the notion of a "driver" seems to have expanded further as now **"permit holders"** for a pilot of autonomous driving have been assigned driver status. Furthermore, options to establish rights and obligations for all traffic participants who have specific obligations for road safety open up a wide range of potentially responsible persons if humans leave the driver's seat and possibly become a 'user-in-charge' or a mere passenger. Based on the reports, however, currently no member State plans to fill the gap left behind by the vanishing human driver with an e-person that, in a more functional approach to criminal justice (see *supra*), would merit a verdict of culpability if an AI driven device causes harm, for instance a car killing a human.

4. Culpability is the crucial criterion for responsibility in criminal cases (as opposed to civil law cases). Consequently, member States **reject the concept of "punishment without fault"** even though they might accept that of **"strict liability"** in torts – with the UK traditionally following a slightly different path on this matter. Driving assistants taking over the steering wheel must have a certain degree of "autonomy" and a linkage to data feed outside the car to be able to react to a specific traffic situation. Autonomy and connectivity however pose risk and may cause harm if an action results in an incident or compromised data distorts the process. Users of an AI driven product cannot fully assess and completely eliminate these risks and, consequently, can in principle not be blamed if harm occurs when complying with all relevant requirements according with the state of the art in science and technology or the user manual or a specific permit etc.

5. AI driven vehicles entering daily lives offer the prospect of more convenience and safety, but carry a certain risk (due to connectivity) of harm occurring without a way of identifying the cause, due to the necessary data stream supplied by others. As things stand today, most member States seem to lack a concept of **"contributory negligence"** for criminal law wherein responsibility is, presumably, shared among several parties for causing harm. Such a notion might gain importance with regard to the connectivity risk, for instance, if a car driven by automation is fed with incorrect map data, which suggests a speed limit of 100 km/h, but in fact the speed limit is 80 km/h and, at the same time, a sensor's functionality is limited and misinterprets traffic signs. In member States, however, where the notion of complicity is very broad, and the contribution of an 'accomplice' does not have to be causal to the result, criminal liability might be far-reaching. It might be advisable to consider whether and how in particular cases the degree of negligence (or the "amount" of the contribution) can be quantified and may influence the sentencing.

IV. Cross-border implications of risk allocation

1. In Europe, cars crossing borders is a ubiquitous phenomenon. Every day thousands of citizens cross borders to reach their working place, go on a holiday, travel on business, or on a visit to family and friends. The commitment of European institutions to provide a legal framework to facilitate cross-border activity and provide legal certainty for its citizens as well as for the industry providing the necessary technology to do so is a crucial element of Europe's strength. The availability of driving automation in one member State will affect all neighbouring States. Firstly, drivers will accustom to automated driving and might even use across-borders where it is not legal. Secondly, the risk of fatal incidents may realize across borders. For instance, if a driver, crossing the Pont de l'Europe (driving from Germany to France over the river Rhine), uses a lane keeping assistant and suffers a stroke in the middle of the bridge, the driving assistant might perfectly steer the car into the Port du Rhin, where it could hit a pedestrian crossing the street. In such a case several issues about the (cross-border) legal implications of driving assistants (employed to operate on their own or in co-operation with humans) have to be acknowledged. AI comes with **new risks**, namely, the autonomy and connectivity risk and dangers emanating from the human-robot-interface. Thus, the question needs to be addressed as to who will bear these risks, or if (and on what conditions) society might accept that, in certain cases and under certain circumstances, even though a particular level of risk needs to

be assumed, no one will be held criminally liable for the sake of the overall social benefit (”socially accepted risk”). These considerations are based on policy decisions in criminal justice, often determined by constitutional law.

2. This question merits special attention if some member States allow **human drivers** to avert attention from traffic when using driving automation, and others do not. The discrepancy has practical implications, as drivers become accustomed to driving automation, and might lead to particular cross-border issues. If, for instance, a car on driving automation, which is fed with incorrect map data and does not realize it crosses a border, speeds and runs over a human, the question arises whether the human driver can be held fully accountable. Or if a car, while legally on driving automation in its country of registration, runs over the citizen of another member State, and that State wishes to prosecute the human driver for manslaughter. Clearly, rules on jurisdiction and mutual legal assistance do provide methods of resolution, and some answers may seem rather easy at first glance, as a driver (or a pedestrian) who crosses a border, enters a different legal regime, and in principle must comply with the relevant domestic law. Whether these are convincing answers is, however, an entirely different matter, in particular, where European citizens have become used to borderless travel. If member States wish to provide sound solutions, the underlying issues ought to be addressed. One problem may be that member States operate with different notions to reflect the fact that not all risk taking is criminal, even if it causes harm.

3. A group of member States does employ the idea of a **“socially accepted risk”** without an explicit legal basis as developed by legal scholars. The idea of a “socially accepted risk” underpins legislation on traffic regulation (e.g. when setting speed limits) or definitions of safety norms (e.g. mandatory airbags) or regulation on the production and regular technical inspections of motor vehicles. Another group of member States **refutes the idea of impunity for certain risk taking,** even if it is, overall, beneficial to society or does not apply it to traffic crimes.

4. Some member States include variations of “socially acceptable risks” in their criminal codes, for instance, “**legally admissible risk”** or **“justified economic risk”**, which all apply if an action is taken in order to achieve a substantial benefit for society. To benefit from this regulation, an actor must do everything within his or her capacity to prevent damage and, in particular, comply with advances in science and technology. The impunity may not apply if

human lives are put in danger or if the actor creates a risk of an ecological or public disaster. Other countries grant impunity during a (scientific or technological) test phase.

V. New forms of crimes

1. Driving automation may make it necessary to consider, in addition to existing rules, new criminal provisions to prevent and punish novel forms of (intentional or negligent) misconduct, in particular related to an impairment of AI or the human-robot interaction which results in harm. For instance, recklessness during production and training of AI driven gadgets or negligence when monitoring a smart product after market entry, or the obstruction of driving automation in various ways or the impairment of human attention necessary for co-operating with AI.

2. The use of driving assistants – replacing human drivers behind the wheel – is expected to modify the driver's liability, the producer's liability, and possibly trigger new regulatory approaches of accountability. Such a development could be a challenge, especially where criminal justice systems substantiate liability with a **faulty human action when using a motor vehicle**, for instance distracted driving while texting, talking on the phone, putting on makeup, or driving intoxicated.

3. Furthermore, in most member States, traffic crimes do **not fall within the schemes of corporate liability**. This may trigger questions as to the scope of producers' liability when driving assistants replace human drivers. Possibly certain serious offences, such as those threatening life and limb, ought to be adapted so that they can apply to the corporate body responsible for the actions of the vehicle. Again one underlying issue is the question of whether (every type of) risk taking should trigger criminal liability (see *supra* B.IV.)

VI. Data as evidence in criminal proceedings

1. Highly-automated cars **generate valuable data that can also be of great interest for law enforcement and criminal investigations**. Against this backdrop, member States acknowledge the need to assess the merit of new rules, for instance, with regard to access and

readability of data. Member States that regulate driving automation require data-event recorders (e.g. a data-storage box) to store relevant data as a rule.

2. Furthermore, driving automation necessitates that driving assistants observe and evaluate the human drivers' ability to co-operate with AI, for instance, by retaking control where necessary (a prominent example is drowsiness detection systems). If highly-automated driving ends in an accident, the question arises whether this data can be used as **evidence in a criminal trial,** in particular, against the human driver, and how to test the **credibility of the systems generating data or the reliability of such data as evidence**. To respond to these questions, most member States want to draw on traditional rules, for instance, the right to bring an expert for the defence or to comment on and "confront" all incriminating evidence. However, classic rules may not be designed to meaningfully test reliability and credibility of this new digital evidence.

3. Member States' authorities already use various **digital analytical tools** to enforce safety on public roads, for instance, "speed cameras" and "radar guns", digital breathalysers, automatic number plate recognition, smart tachographs for trucks, anti-alcohol engine locks. Authorities sometimes also make use of digital evidence generated by systems designed as a consumer service and not as an evidentiary tool to be used in a forensic setting, such as GPS positioning of a vehicle. For most of this evidence, it is as yet unclear how such 'digital testimony' can be challenged meaningfully.

C. Conclusions

1. The way in which driving automation is dealt with by member States reveals different approaches in the employment of AI-driven technology in daily life that creates a paradigmatic human-robot interface that is tangible and visible for citizens:

a) some member States are embracing driving automation, along with its opportunities and risks, while others are more cautious;
b) some member States are striving to clarify the emerging new bundle of responsibility triggered by the use of AI driven vehicles, currently faced by human users ("drivers") in particular, without, however, giving a clear answer on how to close the inevitably emerging

responsibility gap if the human user is (partly) released from liability and, notably, whether someone will assume the burden, and if so, who. Other member States clearly want to retain 'user' or 'operator' responsibility (or at least an assessment on the basis of pilot project rules which in some States establish rigorous liability rules); the issue of introducing a new e-personhood (of the AI driving system) has not been tackled yet;

c) some member States, however, are already focusing on the peculiarities of driving automation, which guarantees more safety, but also carries new risks, in particular, regarding the capacity of automated "decision making" of driving assistants, the need for a certain interconnectivity and the newly emerging human-robot interface with new demands on users, for example, on feasible non-driving activity or responses to take-over requests. Other member States seem to be of the view that the application of traditional legal rules is sufficient, even though they acknowledge the emergence of possible new hazards;

d) some member States acknowledge the new challenges for all different stakeholders (including the state authorities), while others prefer to wait for the development of the relevant technology.

2. Member States, however, agree that – with the onset of driving automation or, at the latest, when "cars drive by themselves" and human drivers have disappeared leaving a responsibility gap behind – there is a need for new regulations with regard to who will be responsible and on what terms. New regulations should, in particular, address:

- new rights and obligations of the relevant actors in a pan-European common approach; by doing so, States ought to assess the fact that, with AI driven systems, non-human actors have entered the scene with the potential capacity to challenge the community's trust in the validity of the law, for instance, if a "robot driving a car" runs over a human without a criminal law response. This might merit a more functional approach in criminal justice, and possibly an evaluation of the option of a e-personhood;
- updates or new concepts of liability, including corporate liability, be it criminal, civil or administrative according to the national legal system;
- reform of traffic offences (which currently focus on human action, and not on AI driven vehicles);
- an evaluation as to what new risks arise from the deployment of AI driven systems and who shall bear them, with particular consideration of possible cross-border risks;

- new evidentiary issues when AI driven systems generate data valuable for criminal investigations. This is the case for evidentiary tools created for fact-finding (such as digital breathalyzers or radar guns used in the member States), but also with regard to data generated during the use of AI, for instance, in driving automation.

3. When considering the member States' answers, the group of experts found that the following issues merit further discussion with regard to prevention, detection, judicial assessment and possible prosecution and punishment of action causing harm when employing AI in human living environments:

A. The employment of AI in living environments probably requires a deeper analysis of basic principles shaping criminal liability in member States today. The traditional notions of criminal responsibility are based on long-standing concepts of personhood, capacity and culpability. With a non-human actor entering public roads, member States might want to consider a more functional approach to criminal justice to sustain the citizens' trust in the validity of the law when a 'robot driving a car' runs over a human or, in an interconnected living environment, harm is caused by many different actors, that, for instance, may feed in incorrect map data, sensor information or have recklessly designed or trained an AI system. Member States might find it worthwhile to test different new approaches for closing the responsibility gap that opens when industrially-produced AI systems gradually replace the human driver in order to provide legal certainty not only to the industry striving to make AI driven vehicles available but also the citizens of Europe who might want to make use of such technology while enjoying protection of life and limb.

B. Driving automation raises many questions on how to effectively protect life and limb in public traffic. One important question is how to modify and adapt criminal provisions to adequately capture accountability for new risks (or lack of risk prevention). These ought be identified (for instance, hacking into software to cause a crash, negligent production and/or training of AI, failure to monitor of a smart product after market entry, obstruction of driving automation by third persons) and compiled in new provisions that aim for due diligence in producing and using driving automation.

C. Member States might like to explore novel evidentiary issues and forensic science developments as a consequence of using AI generated data for criminal investigations and criminal trials. While digital tools have proven helpful to detect and establish criminal action in criminal proceedings in the past, certain indicators suggest a lack of adequate rules to vet the validity of particular digital evidence, generated during driving automation.

ANNEX 1

Strasbourg, 19 May 2019 CDPC(2019)8FIN

EUROPEAN COMMITTEE ON CRIME PROBLEMS

(CDPC)

/

QUESTIONNAIRE CONCERNING ARTIFICIAL INTELLIGENCE AND CRIMINAL JUSTICE (using the example of Automated Driving)

Document prepared by the Working Group of Experts on Artificial Intelligence and Criminal Law,
chaired by Ms Sabine Gless, Professor of Criminal Law and Criminal Procedure, Law Faculty of the University of Basel

www.coe.int/cdpc | dgi-cdpc@coe.int

Introduction

A. Background

In the 21st century technology is rapidly evolving and in recent years has been noticeably driven by the use of Artificial Intelligence (hereafter AI). Long-term technological trends in this domain suggest that various forms of AI will become more and more involved in modern civilian life by operating and engaging in co-operation with humans. The increased presence of AI in everyday life and in various parts of the criminal justice system presents challenging questions to the Council of Europe as a pan-European organisation (see Council of Europe general activities on AI on https://www.coe.int/en/web/artificial-intelligence/home) and to all its member States. Domestic legislation has not always addressed the issue in a systematic way. However, more recently, some countries have adopted specific regulations and certain member States have made substantial progress in their national legislation on driving automation while some have even adopted statutes explicitly governing liability for correct use for the intended purpose.

The Council of Europe committee on criminal problems (CDPC) (https://www.coe.int/en/web/cdpc/home) started its work on AI and criminal law in 2017 and prepared a first document on this topic: a concept paper on "Artificial intelligence and criminal law responsibility in Council of Europe member States - the case of automated vehicles"(https://rm.coe.int/cdpc-2018-14rev-artificial-intelligence-and-criminal-law-project-2018-/16808e64ad). This document (hereafter the Concept Paper) contains the main elements of a project to be implemented over the next few years by the CDPC.

On 28 November 2018, the CDPC organised a Thematic Session on AI and criminal law responsibility where driving automation served as an example for situations where pervasive computing is responding to human needs, the main objectives of which were to:
i. Examine and ascertain the current existing scope and substance of relevant national criminal legislation and international law, using automated driving as an example for AI deployment, as well as determine where and how regulatory powers are established within the competent national public authorities.
ii. Determine where certain conduct has been or should be prohibited and criminalised in relation to the delegation, division or assignment of tasks, functions and behaviours to automated technologies, and the possible cross-border relevance.
iii. Illustrate the findings under ii (see supra) using the case of automated driving: should new principles and norms of attribution and accountability for natural or legal persons be established to uphold Council of Europe Conventions' goals if automated driving (or other Artificial Intelligence deployment) operates across borders.
iv. Examine the scope and substance of an international legal instrument to provide common standards for the criminal law aspects of automated technologies, in particular automated vehicles.

As follow-up to this Thematic Session, the CDPC set up a working group of experts representing member States supported by some scientific experts (hereafter the working group) and tasked them to assist the CDPC in implementing the project activities contained in the Concept Paper. The working group held its 1st meeting on 27 March 2019 and prepared this questionnaire, which is the first output as foreseen in the Concept Paper (see Output 1 on page 8)[1].

[1] **Output 1 (excerpt): 5.1.1 Research project on national criminal law and international legal framework: (a) Activity**: A questionnaire followed by a compilation of responses and analysis; **(b) Reasons**: In order to survey the current regulatory framework for AI, and in particular automated vehicles, key national-level information should be extracted from the member States; **(c) Working methods**: A questionnaire is to be developed and distributed to the relevant ministries (or other entities, as appropriate); the answers will be analysed by an expert or panel of experts.

B. Objectives and scope

Driving automation is a poignant example of **narrow AI**, a bundling of certain techniques already enabling human co-operation with driving systems, i.e. (**ro)bots** that can interact with each other as well as with a human user in order to (temporarily) take over the driver's tasks as a first step. The eventual goal is autonomous driving cars.

The fact that an industry standard distinguishes between different levels of **driving automation** (Norm SAE J3016_201401) facilitates a comparative approach to the possible impact for criminal law, criminal procedure and mutual legal assistance. Of interest here are the transitions from level 2 onward to level 3 and 4 and possibly to level 5. At level 2 a car can execute dynamic driving tasks but the driver must monitor and overrule the system if necessary. At level 3 a driver no longer needs to monitor when the system is activated, but the driver must respond to a takeover request. Level 5 envisages autonomous driving without a human driver. During automated driving, data is automatically generated that could offer relevant information in a criminal trial after a traffic incident.

While driving automation is probably the most prominent example of AI-human co-operation in daily life, other fields are gaining importance (such as medical devices or service robots). The common feature is the ability and necessity to take in information, react and learn from "experience" without human interference. Therefore neither producers and programmers nor users can foresee *all* possible actions of an AI-driven (ro)bot. This means that one cannot reduce to zero the possibility that such a device may also cause harm to others in a particular situation. Among other things, this fact suggests two mutually-exclusive conclusions as to liability for negligence. It could be argued that no one can be held responsible because the machine is acting "on its own"; alternatively, it could be claimed that a producer can foresee harm and therefore should face *de facto* strict liability for the results of a robot's acts.

The CDPC wishes to assist member States with a common approach to a regulatory framework when the many beneficial, yet potentially risky, uses of AI are to be integrated into daily life. One important aspect for criminal justice systems is accountability for harmful consequences. Duly considering the *ultima ratio* of criminal regulation in this complex field, this project focuses only on situations where the level of harm, or the seriousness of the violation of the obligation breached, could or should entail criminal responsibility, and where the use of AI affects criminal justice systems.

C. Example case

This following scenario illustrates some of the challenges arising for criminal law, criminal procedure and mutual legal assistance from ambient intelligent environments (using the example of driving automation):

Imagine that, for the first time, a vehicle equipped with an "autopilot system" can be used legally on highways in your country. The automated driving system must be used in harmony with the authorisation which requires – among other things – that the human driver is ready to take over the steering wheel within 20 seconds. To ensure the driver's fitness to take over, the producer installs a drowsiness detection system monitoring the driver (seating position, face and especially eye movements) and stores the data with a cloud service provider. During the first months of operation of such cars, it turns out that a certain weather phenomenon in your country (be it morning mist, a sandstorm, midday sun or garbage thrown on the roadside) triggers faulty reactions in the driving assistant's system – especially false-braking, i.e. braking for the wrong reason, for instance a plastic bag drifting in the wind. The producer and all component suppliers do their very best to fix the problems. However, it is clear to everyone involved that the cars will need time to adjust to particular local conditions.

Questions *(When answering the questions you may tick more than one box.)*

1. Does your national legislation and/or case law specifically **address criminal liability issues connected to driving *automation***? □

   a) If so, could you please:

   (1) provide, if available, the relevant texts (in English or in French);
   (2) indicate whether criminal responsibility is allocated to a specific person (natural or legal, e.g. *driver, producer, programmer, fleet supervisor, tele-operator etc.)* and on what standard it is based *(i.e. strict liability, negligence, intention).*

   b) If not, will general rules apply in a situation where a driving assistant /"AI" steers a car when the accident happens, and what kind of problems are to be expected?

2. Does the lawmaker in your country plan **legal reforms** with regard to (criminal) liability connected to **driving automation** (Level 3 of driving automation, see supra A.)?

3. Does the lawmaker in your country plan **legal reforms** with regard to **autonomous systems**, e.g. autonomously driving cars on public streets (without a driver present*, Level 5 of driving automation*, see supra A.), like granting an "e-personhood"?

4. Does your law **differentiate criminal liability for lethal incidents** (on public roads) depending on:

   a) **gravity of the breach of law** (e.g. intentional killing, gross negligence, negligence) □

   If so, is a distinction made based on:

   - general criminal law (applicable to all offences, e.g. intention, negligence)? □
   - specific rules on criminal liability for death caused involving the use of a vehicle, i.e. death by dangerous driving, vehicular homicide)? □
   - other? (please explain briefly)

   b) **perpetrator**, if so is a distinction made based on the following categories:

   - driver of a car? □
   - owner, "keeper", "registered user", "registrar"? □
   - producer (e.g. corporate manslaughter)? □
   - other? (please explain briefly)

5. According to your domestic law and/or case law what does ***criminal*** **negligence** resulting in harm require:

   a) gross violation of a duty of care? □
   b) foreseeability? □
   c) preventability? □
   d) (solely) a violation of a duty of care? □
   e) recklessness? □

   If necessary, please provide a short answer.

6. Does your law use the concept of **strict liability** :
   a) in criminal law, i.e. "punishment without guilt"? □
   b) for (administrative) traffic offences, e.g. handing parking tickets to the owner of a car? □
   c) any other ? (please specify).

   Imagine in the example case (see *supra* C.) unfortunately the car hits a human while driving on autopilot and the person dies. It can be established that the car's sensors were defective, but also the braking assistant had a severe software defect.
   It is however impossible to prove which fault caused the accident. Does your national legislation and/or case law address this problem of a criminal **"contributory negligence"**?
   If your system addresses the problem, is it seen as a problem of
   a) theories of causation? □
   b) "complicity" (or rather collaboration in negligence)? □
   c) any other? (please specify).

7. Imagine further that it could be proven that the car's sensors did not pick up the victim, most likely because he/she held a bag at arm's length and the engineers had "tuned out" bag images from the sensors' vision in order to prevent "false braking". In such a case, criminal justice systems may provide an option to forgo criminal prosecution, arguing that in the light of the overall social benefits a particular type of risk taking should not be punished even if harm is caused as long as the person in question does its best to comply with all requirements of safety and security. (Such a notion, for instance, is prevalent when using airbags in cars where although there is a minimal risk that this safety device might open because of a pothole and kill a passenger, it will moreover save lives in many situations.)

   Does your domestic law recognise the notion of a **"societal accepted risk"**?
   If so, how? (please explain briefly).

8. Does your domestic legislation and/or case law address problems of the obtaining, presentation and evaluation of **digital evidence generated during driving** (e.g. evidentiary requirements; requirement for the car producer to provide data,in readable format)? If so, please explain briefly.

9. Are there **problems with digital evidence** stored in a car or at the manufacturer due to
   a) encryption? □
   b) data storage with a cloud service provider or abroad in a third country? □
   c) technology design of data generation? □
   d) any other? (please specify).

10. Imagine in the example case (see *supra* C.) that the driver overrules the drowsiness detection system's suggestion to take a break, because he/she feels awake and a lethal accident happens and the prosecution wants to introduce the drowsiness alert as evidence.
    In your legal system, could the driver challenge the **credibility of the system or the reliability of such evidence** (possibly even in a way that is similar to challenging the credibility of a witness and the reliability of a testimony)?

11. Do authorities in your jurisdiction use **digital analytical tools** to enforce safety on public roads (i.e. use of digital breathalysers or predictive policing/**profiling** to identify high risk drivers)?