COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 28 April 2022

CDPC-AICL(2022)1

EUROPEAN COMMITTEE ON CRIME PROBLEMS (CDPC)

Drafting Committee to elaborate an instrument on Artificial Intelligence and Criminal Law (CDPC-AICL)

Framework document

Directorate General I – Human Rights and Rule of Law

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

Preamble

[…]

Chapter I – Purposes, Scope and Definitions

Article 1 – Purposes

[…]

Article 2 – Scope and Definitions

1. […]

2. For the purposes of this [instrument], the term:

   - “artificial intelligence system” shall mean a machine-based system that is capable of informing or autonomously making decisions using machine and/or human-based data and inputs;

   - “lifecycle” shall mean all phases of existence of an artificial intelligence system between its design and decommissioning;

   - “artificial intelligence provider” shall mean any natural or legal person, public authority or other body that develops an artificial intelligence system or that has an artificial intelligence system developed with a view to putting it into service;

   - “artificial intelligence user” shall mean any natural or legal person, public authority or other body using an artificial intelligence system in his/her/its own name or under his/her/its authority;

   - “artificial intelligence subject” shall mean any natural or legal person whose legal rights are impacted by decisions made or substantially informed as a result of application of an artificial intelligence system;

   - “driving automation” shall mean (reference to different SAE levels or other official document)

   - “highly automated vehicle” shall mean motor vehicle with highly or fully automated driving functions[1], which:
     a. when activated, can control the motor vehicle - including longitudinal and lateral control - to perform the driving task (vehicle control);
     b. is able, during "highly" or "fully automated" driving, to comply with the relevant traffic rules and regulations for operating a vehicle;
     c. can be overridden or deactivated manually by the driver at any time;
     d. is able to identify when there is a need to hand back control to the driver;
     e. is able to indicate to the driver - by means of a visible, audible, tactile or otherwise perceptible signal - the need to retake manual control of the vehicle with a sufficient time buffer before it returns control of the vehicle to the driver; and

[1] Strassenverkehrsgesetz Section 1a(2)

f. indicates that use is running counter to the system description.

Chapter II – Substantive Criminal Law

Section 1: Offences related to Artificial Intelligence Systems (AI Systems)

Title I – Liability and Sanctions

Article 3 – Liability regarding AI Systems

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure criminal liability for an offence established in accordance with this [legal instrument] (Article x to Article x). In particular, domestic criminal legislation must address the accountability gaps arising from the use of AI systems operating autonomously.

2. Each Party shall take the measures necessary to ensure that persons under an obligation for the design, development and application of AI systems can be held liable where the specific features of AI systems, in particular automation or contributory operations, fosters the commission of a criminal offence established in accordance with this legal instrument.

Article 4 – Corporate liability

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this [legal instrument], committed for their benefit by a natural person with an obligation for the design, development and application of AI systems acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:
    a. a power of representation of the legal person;
    b. an authority to take decisions on behalf of the legal person;
    c. an authority to exercise control within the legal person.

2. In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this [legal instrument] for the benefit of that legal person by a natural person acting under its authority.

3. Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.

4. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

Article 5 – Attempt and Aiding or Abetting

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles x through x of the [present legal instrument] with intent that such offence be committed.

Article 6 – Sanctions and Measures

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles x through x are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.

2. Each Party shall ensure that legal persons held liable in accordance with Article x shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

Title II – Offences Violating Obligations Regarding Design, Development and Application of AI Systems

Article 7 – Intentional Violation of Obligations Regarding Design, Development, Application of AI systems

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, violations of obligations under the Committee on Artificial Intelligence framework regarding design, development and application of AI systems, with regard to safety, security (i.e. data security and cybersecurity) and robustness requirements.

2. In particular, measures shall provide for criminal prosecution of "artificial intelligence provider", with regard to the AI systems they are responsible for, concerning a failure to:
    a. monitor the safety or security of such AI system and respond to problems immediately, possibly with software updates;
    b. analyse potential risks and investigate problems reported regarding such AI system with due diligence;
    c. notify competent authority of safety or security defects immediately;
    d. pass on comprehensive and correct information on potential safety or security defects immediately and carry out all testing with due diligence;
    e. recall such AI systems for safety or security reasons;
    f. carry out all software updates with due diligence;
    g. […]

3. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 8 – Reckless Violation of Obligations Regarding Design, Development, Application of AI systems

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when acting recklessly, violations of obligations under the Committee on Artificial Intelligence framework regarding design, development and application of AI systems, with regard to safety, security (i.e. data security and cybersecurity) and robustness requirements.

2. In particular, […]

3. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Title III – Tampering with AI Systems

Article 9 – Data interference

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of data in connection with obligations under the Committee on Artificial Intelligence framework regarding design, development and application of AI systems without right.

2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 10 – System interference

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of an AI System by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing data.

Article 11 – Misuse of AI Systems

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right the production, sale, procurement for use, import, distribution or otherwise making available of:
    a. AI system designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles x through x;
    b. access to an AI system with intent that it be used for the purpose of committing any of the offences established in Articles x through x.

2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles x through x of this [instrument], such as for the authorised testing or protection of an AI system.

Section 2: Offences related to Automated Driving

Title I – Tampering with Vehicle Safety and Security Obligations

Article 12 – Violating Vehicle Safety and Security Obligations

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally:
    a. violating safety or security standards for highly automated vehicles, which are likely to pose a significant risk to a human;
    b. violating information obligations arising for artificial intelligence providers regarding users of highly automated driving or competent authorities for traffic regulation;
    c. […]

2. Each Party shall adopt such legislative and other measures as may be necessary to establish a failure to adequately monitor the performance of highly automated vehicle as criminal offences under its domestic law.

Article 13 – Offences related to Vehicle Type Approval

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of type approval requirements for highly automated vehicles, […]

Title II – Driving-related Offences

Article 14 – Intentional Violation of Driving-related Obligations

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, using a highly automated vehicle:
    a. that is not roadworthy (i.e. in breach of safety or security requirements or obviously not fit for use in the specific situation);
    b. when the "artificial intelligence user" (i.e. human in charge of responding to take-over-request) is unfit or unqualified;
    c. without an "artificial intelligence user" accountable for the AI system in use;
    d. […]

Article 15 – Reckless Violation of Driving-related Obligations

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed recklessly, using a highly automated vehicle:
    a. that is not roadworthy (i.e. in breach of safety or security requirements or obviously not fit for use in the specific situation);
    b. when the "artificial intelligence user" (i.e. human in charge of responding to take-over-request) is unfit or unqualified;
    c. without an "artificial intelligence user" accountable for the AI system in use;
    d. […]

***Include* Article … - Malicious use of Artificial Intelligence Systems for criminal purposes**

(…) or relate to Cybercrime Convention?

Article 16 – Failure to Respond to or Avert a Risk of Serious Injury During Automated Driving

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally or recklessly, the fact that the "artificial intelligence user" (i.e. "driver in charge"):
    a. fails to take reasonable steps to avert a risk of serious injury arising from using a highly automated vehicle, where she/he was aware of such a risk;
    b. operates a highly automated vehicle when unfit or without proper preparation (as defined by domestic law);
    c. due to own unfitness or unpreparedness fails to respond to a take-over-request or other warning of a vehicle due to […]

Article 17 – Failure to Report Serious Safety or Security Issue

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally or recklessly, that the "artificial intelligence provider" or the "artificial intelligence user" (i.e. driver in charge") fails to report a serious safety or security issue arising from driving, where she/he was aware of such an issue.

Article 18 – Sanctions for Breach of Traffic Rules

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that sanctions for breach of traffic rules can be imposed for offences committed during automated driving.

Article 19 – Tampering with Highly Automated Vehicles or Infrastructure (Hacking)

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct, interference with highly automated vehicles, traffic equipment, infrastructures, platforms etc.

Chapter III – Procedural Law

Section 1: Common Provisions

Article 20 – Scope of procedural provisions

1. Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.

2. Except as specifically provided otherwise in Article x, each Party shall apply the powers and procedures referred to in paragraph 1 of this article according to the Cybercrime Convention.

Article 21 – Conditions and Safeguards

1. Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2. Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds

justifying application, and limitation of the scope and the duration of such power or procedure.

3. To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

Article 22 – Offence Notification Requirements

1. Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for a notification to the “artificial intelligence provider” and the “artificial intelligence user” in case a highly automated vehicle performs an operation that, if carried out by a human would amount to an offense.

Section 2: Data from AI Systems for Evidentiary Purposes

Article 23 – Retrieving of Data from AI Systems

1. Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to investigate crimes committed during design, development and application of AI systems.

2. In addition, each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access AI systems when investigating and determining safety or security defects of highly automated vehicles and/or any of the offences established in accordance with Articles x through x of the [present legal instrument].

Article 24 – Production Order

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:
   a. a person in its territory to submit specified data connected to design, development and application of AI systems in that person's possession or control; and
   b. a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

2. In addition, each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order for a person served a note of an Offense Notification based on Article x to receive the data necessary to defend themselves compliant with the rights set out in Article 6 of the European Convention on Human Rights.

3. For the purpose of this article, the terms are to be understood in the same way as in the Cyber Crime Convention.

Article 25 – Using Data from AI Systems

1. Each Party shall adopt such legislative and other measures as may be necessary to enable the testing of trustworthiness of data retrieved from AI systems.

2. In addition, each Party shall ensure defense rights … according to Article 6 of the European Convention on Human Rights.

Chapter IV – International co-operation

Article … – International co-operation

1. The Parties shall co-operate with each other, in accordance with the provisions of this (…) and in pursuance of relevant applicable international and regional instruments and arrangements agreed on the basis of uniform legislation or reciprocity and their domestic law, to the widest extent possible, for the purpose of investigations or proceedings concerning the criminal offences referred to in accordance with this (…), including seizure and confiscation.

2. Exchange of information/evidence in cross-border cases (…)

Article … – Judicial assistance

1. If a Party that makes extradition or mutual legal assistance in criminal matters conditional on the existence of a treaty receives a request for extradition or legal assistance in criminal matters from a Party with which it has no treaty, it may, acting in full compliance with its obligations under international law, and subject to the conditions provided for by the domestic law of the requested member State / party, consider this (…) as the legal basis for extradition or mutual legal assistance in criminal matters in respect of the offences established in accordance with this (…).