COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Strasbourg, 11 June 2025

CDPC(2025)01

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

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

I. Purpose and Scope

Through its Framework Convention on Artificial Intelligence and Human Rights, Democracy, and the Rule of Law (CAI, CETS No. 225), the Council of Europe (CoE) seeks to safeguard human rights, democracy, and the rule of law as AI systems present new opportunities and challenges. This Convention's transversal approach aims at a unified approach of CoE States on the level of principle, providing them with a methodology to assess risk and impact of AI, leaving space for diversity on the legislation level.

The European Committee on Crime Problems (CDPC), tasked by the Committee of Ministers with overseeing and coordinating CoE activities in crime prevention and control, has been called upon to guide member States on AI-related implications within their field. Specifically, the CDPC has been tasked with drafting a legal instrument on criminal liability related to the use of AI, expected by the end of 2025. With its past activities—particularly the "Feasibility Study on a Future Council of Europe Instrument on Artificial Intelligence and Criminal Law (2020)" and preparatory work by its working group on AI and Criminal Law—the CDPC is well-prepared to fulfill this role.

This discussion paper centers on criminal liability and AI, aiming to help member States navigate their obligations under CAI (CETS No. 225), specifically to:

- implement necessary measures in domestic legislation to uphold the principles, rules, and rights in the CAI (Art. 1);
- protect human rights effectively in relation to AI use (Art. 4);
- adopt or maintain measures ensuring accountability and responsibility for adverse impacts on human rights, democracy, and the rule of law arising from activities within the AI lifecycle (Art. 9);
- adopt or maintain measures ensuring that the privacy rights of individuals and the protection of personal data are respected in activities within the AI lifecycle (Art. 11).
- This position paper also considers relevant obligations under the Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols, along with other CoE conventions on criminal law cooperation where applicable.

The objective is to provide a framework for developing national legislation on criminal liability issues arising within the AI lifecycle and to encourage member States to adapt their criminal laws to address situations where AI usage necessitates it, grounded in shared normative principles. The ultimate aim is to establish a common minimum dominator that enhances coherence in criminal liability standards, thus facilitating mutual assistance in criminal matters.

II. Structured approach and principles

The CDPC is entrusted with handling one of the States' key areas of responsibility: crime prevention and crime control. This also means preventing violations of protected legal interests by detecting and investigating criminal offences and prosecuting and punishing their perpetrators. The following structured approach and principles could help navigate member States' obligations under CAI:

1. AI systems used as a tool to commit a crime

In light of CAI’s principles of accountability, transparency, and proportionality, as well as CDPC’s mandate to draft a legal instrument on criminal liability related to AI, existing criminal laws can be evaluated for their capacity to adequately address the potential of AI systems to harm individuals' lives, physical safety, and other well-being, as well as community assets. When AI systems are used merely as tools to intentionally commit established crimes (such as homicide, murder, or theft), existing provisions in domestic criminal justice systems may sufficiently address the criminal conduct. This does not affect the ability of member States to independently expand liability for the use of AI systems in the commission of a crime or consider it as an aggravating circumstance under their criminal laws .

2. AI systems used to cause harm in novel ways

When AI systems are used to cause harm in novel ways - either through actions not yet punishable under member States’ domestic systems or by leveraging technology to expand the scope and impact of punishable conduct both in scope and impact, specific concerns arise. These include, but are not limited to:

- **Technology-facilitated violence (e.g. against women and girls, TFVaWG)**: This includes using deepfakes of a person’s video, voice, or image for purposes such as sexual exploitation, nudity, advertising, or other commercial uses, with the intent to undermine their moral integrity or to gain an undue advantage of any kind. Such actions involve the dissemination, display, or transfer of their body image or voice generated, altered, or recreated using AI systems.
- **Online sexual grooming using AI systems**: This involves AI-enabled manipulation or deception to initiate contact with a child with the intent to persuade or coerce the individual into producing pornographic material in which a minor is depicted or appears;
- **Distribution of “Dark AI”**: This refers to AI systems specifically engineered for malicious purposes, such as hacking, cracking, or other cyberattacks, as well as AI designed to target critical infrastructure, create situations of serious public security risks or with the intention of facilitating the commission of any crime; including systems that operate autonomously, i.e. without human intervention

3. Bona fide use of AI resulting in harm

When the bona fide use of AI systems leads to harm due to the inherent risk of unforeseeable actions, such as in cases where:

- a chatbot slanders an individual due to an AI hallucination,
- an accident is caused by a self-driving car failing to identify a sled accidentally crossing a highway, or
- high-frequency trading systems inadvertently engage in market manipulation,

member States may wish to discuss a harmonised approach in criminal law to establish a threshold for defining criminal negligence or, alternatively, a narrowly defined exemption from liability without prejudice to possible administrative or civil liabilities.

4. AI systems designed, trained, or deployed in violation of CAI obligations

When AI systems are designed, trained, or deployed in violation of CAI obligations, member States may wish to consider a harmonised approach in criminal law to penalise non-compliance with these obligations, particularly if the non-compliance with requirements lead to incorrect, incomplete, hidden or misleading information that might affect human rights, democracy and the rule of law. Some situations may be those related to:

- accountability, transparency, and non-discrimination in the use of training data; and
- respect for copyright and privacy rights in obtaining training data and training AI systems?

Additionally, the putting into service, produces, acquires for their use, imports or, in any way, provides to third parties or the use of an AI system that is prohibited by its national or European legislation could be considered as an offence.

5. Principle of legality

Clear legislation on criminal activities within the lifecycle of AI systems should, on one hand, respect Article 7 of the ECHR, which states that no one shall be held guilty of a criminal offense for any act or omission that did not constitute a criminal offense under national or international law at the time it was committed, and, on the other hand, protect the fundamental rights, values, and freedoms enshrined in the European Convention on Human Rights.

III. Legal approaches/frameworks for establishing criminal liability

The working group's feasibility study (see *supra* I.) as well as groundwork of comparative criminal law illustrate that member States' criminal justice systems allow for different legal approaches and frameworks to establish criminal liability in the different situations where activities within the lifecycle of AI systems ought to be punished.

First, member States must make a general decision regarding the type of framework they desire for developing national legislation to address punishable activities within the lifecycle of AI systems. Subsequently, they can determine which legal approach would best achieve the ultimate objective of establishing a framework for adequate national legislation.

IV. Need for specific legislation

Regarding the various legislative response options, several issues arise, particularly whether member States consider it necessary to adopt specific legislation in light of the new obligations arising from the CAI.

Need for legislation due to bona fide use of AI Systems

One question is whether member States want to adopt specific measures to address the "negligence dilemma" resulting from the autonomous actions of AI systems, in particular considering the principle of proportionality. This could involve measures that ensure that all parties with duties in the lifecycle of an AI system can be held adequately liable, such as:

- providing for enhanced criminal liability where features of AI systems, particularly automation or contributory operations, foster the commission of a criminal offense, or
- granting a narrowly defined impunity in cases of relevant contributory liability or socially accepted risks, or
- other measures seen as appropriate.

Need for Legislation due to tech-facilitation of high-scale crime ("Dark AI systems")

A similar question arises regarding the capacity of AI systems to act autonomously 24/7, creating the potential to replace entire criminal organisations with a single software architecture that continuously deepfakes or hacks on demand (Crime-as-a-Service as a business model). This increases the risk for individuals who may fall victim to fraud, privacy violations, unauthorized use of images, infringements on intellectual or industrial property, defamation, manipulation of the electoral process, or misleading courts in criminal trials.

The question is whether such tech-facilitation requires a specific response from criminal law that targets criminals providing or acquiring these services, or whether "Dark AI" can be addressed using traditional legal tools, such as imposing harsher penalties during sentencing.

Need for Legislation with regard to the principle of legality

As a general issue, the question arises whether member States should adopt new legislation in order to uphold the principle of legality as enshrined in Article 7 of the ECHR and in their respective domestic laws.

Continue without specific legislation

Alternatively, member States could choose to continue without specific legislation and rely on their traditional body of law - statutes and case law built on rules and cases addressing the (negligent) use of machines by humans, often found in criminal product liability. However, in doing so, they must ensure that they effectively protect human rights related to the use of AI (Article 4) and have measures in place to ensure accountability and responsibility for adverse impacts on human rights, democracy, and the rule of law resulting from activities within the lifecycle of AI systems (Article 9). They must also ensure that privacy rights of individuals and their personal data are protected in relation to activities within the lifecycle of AI systems (Article 11).

Specific exemptions from criminal liability, such as "Dual use technology"

As pointed out above, AI systems hold great potential that can benefit individuals and society as a whole but also can cause harm. In the light of the benefits of AI systems and the principle of proportionality, member States, before establishing new criminal liability, may want to consider specific exemptions from criminal liability, also avoiding the risk of widespread criminalization that could stifle AI development. Dual use technology could be a situation that merits such an exemption.

Questionnaire

A.

1.

Does your national legislation and/or case law specifically address criminal liability or crimes connected to artificial intelligence?
If so, could you please:
(1) provide, if available, the relevant texts (in English or in French);
(2) indicate whether criminal responsibility is attributed to a specific person (natural or legal, e.g., driver, producer, programmer, fleet supervisor, tele-operator, etc.) and what standard it is based on (i.e., strict liability, negligence, intent).
If not, will general rules apply in situations where crimes are committed, facilitated, enhanced, or aided by artificial intelligence?

2.

What general rules are applied in your law when AI systems (as defined in Article 2 of the CAI, ETS No. 225) are used as tools for the intentional commission of criminal offences (such as murder, manslaughter, or theft)?

3.

According to your domestic law and/or case law, can the use of AI systems be considered an aggravating circumstance?

B.

1.

Does the legislator in your country plan legal reforms regarding (criminal) liability and crimes related to AI?

2.

Does the legislator in your country plan legal reforms concerning aggravating circumstances when a crime is committed, facilitated, enhanced, or aided by the use of AI systems?

3.

Would your legislator address the new challenges of effectively protecting rights put at risk by the use of AI systems through measures other than adopting new criminal laws? If so, how?

C.

1.

Does your law address the use of specific AI technologies for committing crimes, e.g., the use of deepfakes in certain contexts (such as sexual deepfakes, online sexual grooming, or during electoral processes), the use of autonomous drones to kill someone, or specific forms of fraud?

2.

Is the use of AI considered an aggravating circumstance, particularly in cases involving:
☐ sexual deepfakes
☐ online sexual grooming
☐ electoral processes
☐ use of autonomous drones to kill someone
☐ fraud of notorious importance
☐ other: ………………………

3.

Does the legislator in your country plan legal reforms concerning the development of applications that facilitate the production of (sexual) deepfakes, or the use or dissemination of (sexual) deepfakes?

4.

Based on your national context and legal developments, are there any other behaviours or activities involving artificial intelligence that your authorities consider should be criminalised in the future? If so, please describe the conduct and, if possible, explain the rationale.

D.

1.

Do you see a need for a new type of offence related to *dark AI*?
(This refers to AI systems specifically engineered for malicious purposes, such as hacking, cracking, or other cyberattacks, as well as AI designed to target critical infrastructure, create serious public security risks, or facilitate the commission of any crime.)

2.

Do you see a need for a new type of offence to criminalise the placing on the market, putting into service, production, acquisition for personal use, importation, or provision to third parties - in any form - of an AI system that is prohibited under national or European legislation?

E.
Does the legislator in your country plan legal reforms concerning the protection of copyright in connection with the use of AI (e.g., due to web scraping, web harvesting, or data extraction from websites to train large language models)?

F.
Do you see a need to adopt specific measures to address the "negligence dilemma" arising from the autonomous actions of AI systems?

G.
1.
Do you see a need for the creation of an international instrument (*Convention on AI and Crimes*) similar to the Budapest Convention on Cybercrime, which would define and criminalise acts that can be committed, facilitated, enhanced, or aided through AI systems?

2.
In your view, should such an international instrument (*Convention on AI and Crimes*) include the following elements?

□ definitions

□ procedural provisions,

☐ jurisdiction provisions

☐ extraditions and mutual assistance issues

☐ problems with digital evidence

☐ collaboration of the digital AI platforms with the prosecution of the crimes

☐ other issues ……………………………………………………………………………………………………

Do you agree that the definitions should align with those in the AI Act?

3.
Which of the above issues do you consider the most urgent to address in relation to AI and criminal law?

4.
Are there any examples of national case law or investigative practice (e.g., criminal investigations, prosecutorial assessments) involving crimes committed or facilitated by artificial intelligence? If yes, please summarise the case(s) or describe the issues, if possible.

5.
Would you prefer the adoption of a single global instrument addressing AI and criminal law, or do you think that specific pieces of legislation should be adopted?